Julie Hess, Partner
Cybersecurity & Data Privacy Team
1650 Market Street, 36th Floor
Philadelphia, Pennsylvania 19103
jhess@constangy.com
Telephone: 610.416.9236
www.constangy.com
Emergency: BreachResponse@constangy.com
Hotline: 877-382-2724 (877-DTA-BRCH)

January 21, 2025

VIA EMAIL

Attorney General Anthony G. Brown
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Notification of Data Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith & Prophete, LLP represents Universal Lenders, LLC ("Universal"), a company located in Oak, Park, Illinois that specializes in servicing promotional programs for dealers who sell extended warranty service contracts and other protection products for automobiles, recreational vehicles, boats, or motorcycles by collecting payments from warranty holders and maintaining and servicing the associated payment account until it is paid off, in connection with a data security incident described in greater detail below. Universal takes the protection of all information within its possession very seriously and has taken measures to reduce the likelihood of a similar incident reoccurring. The purpose of this letter is to notify you of the incident in accordance with Maryland's data breach notification statute, Md. Code Ann., Com. Law § 14-3501 et seq.

1. **Nature of the Security Incident**

On November 7, 2024, Universal experienced a network disruption and immediately initiated an investigation of the matter with the help of independent cybersecurity experts to assist with the process. On December 5, 2024, the investigation determined that certain files were accessed and / or acquired without authorization. Universal then undertook a comprehensive review of those files and, on or about January 14, 2025, learned that some personal information of individuals contained within the potentially affected data. Please note that Universal has no evidence of the misuse, or attempted misuse, of any potentially impacted information.

2. **Number of Affected Maryland Residents & Information Involved**

The incident involved personal information for approximately one hundred nineteen (119) Maryland residents. The information involved in the incident may differ depending on the individual but may include the following for affected Maryland residents: Social Security number, financial account number, or driver's license.

3. **Notification to Affected Individuals**

On January 21, 2025 notification letters were sent to affected Maryland residents by USPS First Class Mail.

The notification letter provides resources and steps individuals can take to help protect their information. The notification letter also offers complimentary identity protection services to each individual whose Social Security numbers was affected by this event, including credit monitoring, dark web monitoring, $1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. A sample notification letter, or a substantially similar version thereof, is enclosed.

4. **Measures Taken to Address the Incident**

Upon discovering this incident, in addition to taking the steps described above, Universal took steps to secure its systems and launched an investigation to learn more about what happened and what information could have been affected. Universal took immediate steps to evaluate and improve the security of its systems and will continue to evaluate additional protections that can be put into place to supplement its existing security policies and procedures.

Universal has established a toll-free call center through IDX to answer questions about the incident and address related concerns. Finally, Universal notified the potentially affected individuals and provided them with steps they can take to protect their personal information and reported the incident to nationwide consumer reporting agencies (i.e., Equifax, Experian, and Transunion).

5. **Contact Information**

If you have any questions or need additional information regarding this incident, please do not hesitate to contact me at JHess@constangy.com or 610.416.9236.

Sincerely,

Julie Hess

Julie Hess
Partner, Constangy Cyber Team

JH:mff
Encl.: Sample Notification Letter

Univeral Lenders, LLC
P.O. Box 989728
West Sacramento, CA 95798-9728

Enrollment Code: <<ENROLLMENT>>
To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://app.idx.us/account-creation/protect

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

January 21, 2025

Subject: Notice of Data <<Variable Text 1: Security Incident/Breach>>

Dear <<First Name>> <<Last Name>>:

I am writing to inform you of a recent data security incident that may have affected your personal information. Universal Lenders, LLC ("Universal") takes the privacy and security of all information within its possession very seriously. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your personal information.

What Happened. On November 7, 2024, Universal experienced a network disruption and immediately initiated an investigation of the matter with the help of independent cybersecurity experts to assist with the process. On December 5, 2024, the investigation determined that certain files were accessed and / or acquired without authorization. Universal undertook a comprehensive review of those files and, on or about January 14, 2025, learned that some of your personal information was contained within the potentially affected data which is the reason for this notification. Please note that Universal has no evidence of the misuse, or attempted misuse, of any potentially impacted information.

What Information Was Involved. The information may have included your name and <<Variable Text 2: Data Elements>>.

What We Are Doing. As soon as Universal discovered this incident, we took the steps described above and implemented measures to enhance security and minimize the risk of a similar incident occurring in the future. We are also offering you complimentary identity protection services through IDX, a leader in consumer identity protection. These services include <<12/24>> months of credit monitoring[1], dark web monitoring, a $1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. The deadline to enroll in these services is April 21, 2025.

What You Can Do. You can follow the recommendations on the following page to help protect your personal information. You can also enroll in the complementary services offered to you through IDX by using the enrollment code provided above.

[1] To receive credit monitoring services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

For More Information. Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call 1-877-720-8806 Monday through Friday from 8 am – 8 pm Central Time, except holidays. We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience this may cause.

Sincerely,

Universal Lenders, LLC

Steps You Can Take to Help Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax	**Experian**	**TransUnion**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-800-916-8800
www.equifax.com	www.experian.com	www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission	**Maryland Attorney General**	**Oregon Attorney General**
600 Pennsylvania Ave, NW	200 St. Paul Place	1162 Court St., NE
Washington, DC 20580	Baltimore, MD 21202	Salem, OR 97301
consumer.ftc.gov	www.marylandattorneygeneral.gov/Pages/CPD	www.doj.state.or.us/consumer-protection
877-438-4338	888-743-0023	877-877-9392

California Attorney General	**New York Attorney General**	**Rhode Island Attorney General**
1300 I Street	The Capitol	150 South Main Street
Sacramento, CA 95814	Albany, NY 12224	Providence, RI 02903
www.oag.ca.gov/privacy	ag.ny.gov	www.riag.ri.gov
800-952-5225	800-771-7755	401-274-4400

Iowa Attorney General
1305 E. Walnut Street
Des Moines, Iowa 50319
www.iowaattorneygeneral.gov
888-777-4590

NY Bureau of Internet and Technology
28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
212.416.8433

Washington D.C. Attorney General
400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov/consumer-protection
202-442-9828

Kentucky Attorney General
700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
502-696-5300

NC Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov/protectingconsumers/
877-566-7226

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.