



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

RECEIVED

DEC 18 2025

CONSUMER PROTECTION
DIVISION

Brittany R. Bickel
Office: (267) 930-1129
Fax: (267) 930-4771
Email: bbickel@mullen.law

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

December 18, 2025

VIA E-MAIL

Office of the Idaho Attorney General
Consumer Protection Division
P.O. Box 83720
Boise, ID 83720-0010
E-mail: consumer_protection@ag.idaho.gov

Re: Notice of Data Event

To Whom It May Concern:

We represent 700Credit, LLC ("700Credit") located at 26555 Northwestern Highway, Suite 301, Southfield, MI 48033. 700Credit provides services to dealerships nationwide to assist with consumer financing options. We write on behalf of 700Credit and its dealership clients to provide a courtesy notice to your office of an incident that may affect the security of certain personal information relating to 38,405 Idaho residents. By providing this notice, 700Credit does not waive any rights or defenses regarding the applicability of Idaho law, the applicability of the Idaho data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or around October 25, 2025, 700Credit became aware of suspicious activity within its web application and immediately launched an investigation, with the assistance of third-party computer forensic specialists, to confirm the full nature and scope of the activity. The investigation determined that certain records in the web application relating to customers of its dealership clients were copied without authorization. 700Credit thereafter undertook a thorough review of the potentially impacted records to determine what information was included in the records, to whom the information relates, and to identify contact information for purposes of providing notifications to its clients. On November 21, 2025, 700Credit began notifying impacted dealership clients of the event. 700Credit then took steps to retain a notification vendor and confirm approvals to issue notices on behalf of its dealership clients. That process recently concluded.

The information that was subject to unauthorized acquisition varies by individual but includes name, address, Social Security number, and date of birth.

Notice to Idaho Residents

On or about December 22, 2025, 700Credit will begin providing written notice of this incident to 38,405 Idaho residents on behalf of its dealership clients. 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 becoming aware of the event, 700Credit moved quickly to investigate and respond to the incident, assess the security of 700Credit systems, and identify potentially affected individuals. Further, 700Credit notified federal law enforcement and the Federal Trade Commission regarding the event. 700Credit is continuously working to enhance its existing security measures with additional safeguards and training to its employees. 700Credit is providing access to credit monitoring services for 12 months, through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, 700Credit 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. 700Credit 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-1129.

Very truly yours,



Brittany R. Bickel of
MULLEN COUGHLIN LLC

BRB/lac
Enclosure

EXHIBIT A



[TRANSUNION RETURN MAIL ADDRESS]

<<Date>>

<<Name 1>> <<Name 2>>:
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

NOTICE OF DATA BREACH

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

700Credit, LLC ("700Credit") provides services to dealerships nationwide to assist with consumer financing options and is writing to notify you of an incident that may affect some of your information. Although we have no evidence of any identity theft or fraud occurring as a result of this event, this letter provides details of the incident, our response, and resources available to you to help protect your information, should you feel it is appropriate to do so.

What Happened? On or around October 25, 2025, 700Credit became aware of suspicious activity within our web application and immediately launched an investigation, with the assistance of third-party computer forensic specialists, to confirm the full nature and scope of the activity. The investigation determined that certain records in the web application relating to customers of our dealership clients were copied without authorization. 700Credit thereafter undertook a thorough review of the potentially impacted records to determine what information was included in the records and to identify contact information for purposes of providing notifications. That review recently concluded.

What Information Was Involved? Our investigation determined the following types of information related to you was present in the involved records: your name, address, date of birth, and Social Security number. At this time, we have no indication that your information was subject to actual or attempted misuse as a result of this incident and are providing this notice out of an abundance of caution.

What We Are Doing. Data privacy and security are among 700Credit's highest priorities, and there are extensive measures in place to protect the information in our care. Upon becoming aware of the incident, we promptly commenced an investigation with the assistance of third-party computer forensic specialists to confirm the nature and scope of this incident. This investigation and response included confirming the security of our network environment, which was not impacted by this incident, reviewing the content of relevant records for sensitive information, and notifying potentially impacted individuals. As part of our ongoing commitment to the privacy of information in our care, we are reviewing our policies, procedures and processes related to the storage and access of personal information to reduce the likelihood of a similar future event.

As an added precaution, we are also offering you [Variable Text] months of access to credit monitoring services, through Cyberscout, a TransUnion company, at no cost to you. Please note, you must enroll by following the attached enrollment instructions as we are not able to enroll in these services on your behalf.

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. Please also review the information contained in the attached **STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION**. There you will also find more information regarding the complimentary credit monitoring services we are making available to you.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please contact us at 833-586-1820, Monday through Friday, from 8 am – 6pm Eastern (excluding major U.S. holidays).

Sincerely,
700Credit, LLC

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

In response to the incident, we are providing you with access to **Single Bureau Credit Monitoring** services at no charge. These services provide you with alerts for <<service length>> months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

How do I enroll in the free services?

To enroll in Credit Monitoring services at no charge, please log on to <<URL>> and follow the instructions provided. When prompted please provide the following unique code to receive services: <CODE HERE>

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

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. Should consumers wish to place a fraud alert, they may do so by contacting 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, they may do so by contacting 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/data-breach-help

1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, 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, 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.