KEAN | MILLER LLP

MONICA MANZELLA, SENIOR COUNSEL
PH 504-585-3050
MONICA.MANZELLA@KEANMILLER.COM

May 12, 2025

Via Email and Certified Mail
9589 0710 5270 2173 9889 77
Attorney General's Office
Consumer Protection Division
P.O. Box 83720
Boise, ID 83720-0010
consumer_protection@ag.idaho.gov

Re: Database Security Incident Report
File No. 30951.10

Dear Attorney General Labrador:

My firm represents Used Bikes Direct, LLC ("UBD"), a motorcycle retail company doing business at 10939 Airline Highway, Baton Rouge, Louisiana 70816. This correspondence concerns a data breach that affected 6 Idaho residents.

Beginning on or around January 17, 2025, an online account held by UBD for the credit platform (CRSS Credit API) used by UBD for consumer credit reports ("Portal") was compromised by a malicious actor. Through the Portal, the malicious actor was able to view historical consumer credit reports of UBD customers and the personal information of the customers whose reports were accessed. CRS discovered the compromise in March 2025 and UBD was provided with the list of impacted individuals on or around March 28, 2025. On April 4, 2025, UBD determined the individuals' information that may have been accessible to the threat actor, which is information that may appear on a credit application or credit report. The personal information may have included: name, birth date, Social Security Number, address, salary information, and credit rating.

All reports accessed during the breach constituted soft inquiry pre-qualification reports that should not impact an individual credit score; no new reports were pulled during the intrusion. For a limited number of individuals, UBD determined that the threat actor had attempted to submit credit pre-approval forms using the information accessed. No loans have been underwritten nor hard credit inquiries made and all such applications for credit submitted to UBD were voided. To date, UBD is not aware of any other instances of identity theft attempted with this information.

CRS conducted a thorough investigation to confirm that the unauthorized access was solely through the wrongdoer obtaining and using UBD's authorized log-in and password, and CRS immediately blocked further access to that account. The security and privacy of information contained within UBD's systems is a top priority, and UBD is also taking additional measures to protect this information. UBD has already implemented additional authentication procedures, including multi-factor authentication,

implemented additional training requirements, and is conducting thorough reviews for steps to further implement additional safeguards, policies, and procedures relating to data privacy and security.

UBD is offering affected consumers 12 months of credit monitoring and identity theft protection services through TransUnion. UBD has also established a dedicated, toll-free call center to answer questions that individuals may have. A copy of the notice to be sent via U.S. Mail to affected persons on May 12, 2025 is included with this letter.

It is our understanding that this correspondence should meet the requirements for notice under Idaho's Security Breach Notification Law. However, if anything further is needed, please contact me at monica.manzella@keanmiller.com or (504) 620-3356 or contact Jessica Engler at jessica.engler@keanmiller.com or (504) 620-3361.

Very truly yours,

KEAN MILLER LLP

Monica J. Manzella
Jessica C. Engler

MJM/cb
Enclosure

UsedBikes Direct
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS923

0000200

1_0000200

[redacted]

May 9, 2025

Notice of Data Breach

Dear [redacted],

We are sending this letter to you as part of Used Bikes Direct, LLC's ("**UBD**") commitment to protecting your privacy, security, and confidential information. We take information privacy very seriously, and it is important to us that you are made fully aware of any potential privacy issue. The purpose of this notice is to inform you of an incident that affected UBD that involved your private or personal information, to provide you with information about the incident, our response to it, and additional steps you may take to better protect your private or personal information, should you feel it appropriate to do so.

What Happened
Beginning on or around January 17, 2025, an online account held by UBD for the credit platform (CRSS Credit API) used by UBD for consumer credit reports ("Portal") was compromised by a malicious actor. Through the Portal, the malicious actor was able to view historical consumer credit reports of UBD customers and the personal information of the customers whose reports were accessed. CRS discovered the compromise in March 2025 and UBD was provided with the list of impacted individuals on or around March 28, 2025. On April 4, 2025, we determined that your information may have been accessible to the threat actor. All reports accessed during the breach constituted soft inquiry pre-qualification reports that should not impact an individual credit score; no new reports were pulled during the intrusion.

For a limited number of individuals, UBD determined that the threat actor had attempted to submit credit pre-approval forms using the information accessed. No loans have been underwritten nor hard credit inquirites made and all such applications for credit submitted to UBD were voided. You will be contacted separately if your information was used in such a manner. To date, we are not aware of any other instances of identity theft attempted with this information, but UBD strongly encourages all customers to be vigilent in protection of their information.

What Information Was Involved
The personal information that may have been obtained by the third party is information that may appear on a credit application or credit report. The personal information may have included: your name, birth date, Social Security Number, address, salary information, birthday, and credit rating.

What We Are Doing
CRS conducted a thorough investigation to confirm that the unauthorized access was solely through the wrongdoer obtaining and using UBD's authorized log-in and password, and CRS immediately blocked further access to that account. The security and privacy of information contained within UBD's systems is a top

safeguards, policies, and procedures relating to data privacy and security. We are sending you this notice so that you can, in addition to our efforts, act as you see fit to protect your identity. Please see the enclosed "Additional Resources" for additional information.

As part of this effort, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for twelve (12) 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 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 for the free services?
To enroll in Credit Monitoring services at no charge, please log on to https://bfs.cyberscout.com/activate and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted] 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.

What You Can Do
UBD encourages you to remain vigilant against incidents of identity theft and fraud, to monitor your account statements and free credit reports, and to watch for suspicious or unauthorized activity. If you are contacted by the malicious actor, we recommend that you do not engage with this group. If you are aware of or otherwise suspect or discover that your information has been disclosed and/or used inappropriately, please notify your local law enforcement, your state attorney general, or consumer protection agency. For more information on additional steps you can take to protect this information, please see the "Additional Resources" pages that follow this letter and sign up for the offered credit monitoring.

More Information
Should you have any questions or need additional information, please Contact our Customer Service Line at 469-985-2560.

We take very seriously our role of protecting your private and personal information. Unfortunately, cyberattacks continue to increase at an alarming rate and no organization is completely immune despite the security initiatives taken to prevent such attacks. We have taken and will continue to take steps to maximize our security, minimize the impact of this attack, and prevent a reoccurrence in the future.

Please keep this notice for your records.

Sincerely,

Robert Hyde

Robert Hyde III

Used Bikes Direct, LLC
10939 Airline Highway
Baton Rouge, LA 70816

Additional Resources

Order Your Free Credit Report. You are entitled to receive your credit report from each of the three national credit reporting agencies once per year, free of charge. You may obtain your free annual credit report by visiting www.annualcreditreport.com, by calling toll-free at 1-877-322-8228, or completing the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The credit reporting bureaus provide credit reports only through the website, toll-free number, or request form. Do not contact the three credit bureaus individually.

When you receive your credit report, review it carefully. Errors may be a warning sign of potential identity theft. Here are a few tips of what to look for:

Look for accounts that you did not open.

Look in the "Inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names. The credit bureau will be able to tell if this is the case.

Look in the "Personal Information" section for inaccuracies in information (such as home address or Social Security Number).

If you see anything you do not recognize, call the credit bureau at the telephone number on the report. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so that the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity. You have a right to obtain a copy of the police report, which you may need to provide to creditors to clear up your records.

We encourage you to take advantage of these protections and remain vigilant for incidents of fraud and identity theft, including monitoring your credit reports and account statements.

Fraud Alerts. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file at no cost for 1 year. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit with a fraud alert set, the merchant must take additional steps to verify the identity of the applicant. If you are a victim of identity theft, you are entitled to an extended fraud alert for 7 years.

You can report potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Security Freeze. You have the right to place a security freeze on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. Please be aware that using a security freeze to control 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 of application you make regarding a new loan, credit, mortgage, or other account involving the extension of credit.

You can place, temporarily lift, or permanently remove a security freeze on your credit report online, by phone, or by mail. You will need to provide certain personal information, such as address, date of birth, Social Security number, proof of current address, or copy of state-issued identification card to request a security freeze and may be provided with a unique personal identification number (PIN) or password, or both,

that can be used by you to authorizer the removal or lifting of the security freeze. Information on how to place a security freeze with the credit reporting agencies is also contained in the links below:

https://www.equifax.com/personal/credit-report-services/
https://www.experian.com/freeze/center.html
https://www.transunion.com/credit-freeze

As of June 30, 2023, the credit bureaus allow you place a credit freeze through online, physical mail, and phone numbers, and request that you provide the information listed below. Where possible, please consult the websites listed above for the most up-to-date instructions.

Reporting Agency	Online	Physical Mail	Phone Number
Equifax	***Freeze request may be submitted via your myEquifax account, which you can create here*:** https://my.equifax.com/consumer-registration/UCSC/#/personal-info	***The Equifax Freeze Request Form may be found here:*** https://assets.equifax.com/assets/personal/Security_Freeze_Request_Form.pdf ***and mailed to:*** Equifax Information Services LLC P.O. Box 105788 Atlanta, GA 30348-5788	888-298-0045
Experian	***Freeze request may be submitted here*:** https://www.experian.com/ncaconline/freeze	***Mail the request to:*** Experian Security Freeze P.O. Box 9554 Allen, TX 75013	888-397-3742
TransUnion	***Freeze request may be submitted via your TransUnion account, which you can create here:*** https://service.transunion.com/dss/orderStep1_form.page?	***Mail the request to:*** TransUnion P.O. Box 160 Woodlyn, PA 19094	888-909-8872

Fees associated with placing, temporarily lifting, or permanently removing a security freeze no longer apply at nationwide consumer reporting agencies.

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 FTC, or their state attorney general. The FTC 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 FTC 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. A checklist of the steps listed above and links to forms and other helpful information can be found on the site at https://IdentityTheft.gov/steps.

Federal Trade Commission and State Attorneys General Offices. If you believe that you are the victim of identity theft or have reason to believe that your personal information has been misused, you should immediately contact local law enforcement authorities, the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission** to learn more about how to protect yourself from identity theft at Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

For Connecticut Residents: You may contact the Connecticut Attorney General's Office, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Maryland Residents: You may contact the Maryland Attorney General's Office, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, https://www.marylandattorneygeneral.gov/.

For New Mexico Residents: Consumers have rights pursuant to the Fair Credit Reporting Act (FCRA), 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, right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the FCRA, the consumer reporting agencies 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 FCRA not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the FCRA. We encourace consumers to review their rights by visiting www.consumerfinance.gov/f/201504_cfpb_summary_yourrights-under-fcra.pdf, or by writing to Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York Residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224, 1-800-771-7755, https://ag.ny.gov. You may also contact the New York Department of State Division of Consumer Protection, 99 Washington Avenue, Ste. 650, Albany, NY 12231, 1-800-697-1220, www.dos.ny.gov.

For North Carolina Residents: You may contact the North Carolina Attorney General's Office, 9001 Mail Service Centre, Raleigh, NC 27699-9001, 1-919-716-6000, 1-877-566-7226, www.ncdoj.gov.

For Oregon Residents: We encourage you to report suspected identity theft to the Oregon Attorney General at Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096.

For Rhode Island Residents: You may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General at Rhode Island Attorney General's Office, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov. For security incidents generally, you have the right to obtain a copy of a police report. This incident impacted 1 Rhode Island resident.

Reporting Identity Theft and Obtaining a Police Report.

For Iowa Residents: You are advised to report any any suspected identity theft to law enforcement or to the Iowa Attorney General. The Iowa Attorney General may be contacted at Office of the Iowa Attorney General, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319, 515-281-5926, 888-777-4950, www.iowaattorneygeneral.gov.

For Oregon Residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commision, and the Oregon Attorney General.

For Vermont Residents: If you do not have internet access but would like to learn more about how to place a secuirty freeze on your credit report, contact the Vermont Attorney General's office at: 800-649-2424 (toll-free in Vermont), 802-656-3183.

For West Virginia Residents: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.