

## **Notice of Data Security Event**

Dillon County (“the County” or “we”) is issuing notice of a recent incident involving potential unauthorized access to personal or identifying information maintained by the County. Protecting the confidentiality, privacy, and security of the information entrusted to us is a top priority, and we are acting quickly and diligently to address this matter. After an extensive investigation conducted in coordination with third-party computer forensic specialists, it was determined that certain personal information may have been involved in the incident. We are writing to keep our County community informed so individuals may take steps to protect their information, should they feel it is appropriate to do so.

### **What Happened?**

On or about November 3, 2025, the County became aware of unusual computer activity resulting in disruptions to certain systems and resources. In response, the County immediately took steps to secure its environment while minimizing system disruptions and notified law enforcement. The County also launched an investigation with assistance from cybersecurity specialists to determine the nature and scope of the activity. The investigation subsequently determined certain County systems were accessed without authorization between November 2, 2025 and November 3, 2025, and during this time certain files were copied and potentially viewed. The County is not currently aware of any identity theft or fraud as a result of this incident.

### **What information was involved?**

The relevant files could involve the following types of personal or identifying information: name, Social Security number, date of birth, government identification or driver’s license information, financial account information, payment card information, username & password, and digital signature, if stored on the affected County systems.

### **What are we doing?**

The County takes the confidentiality, privacy, and security of information in its care seriously. Upon learning of this incident, the County took steps to implement additional safeguards and review our policies and procedures relating to data privacy and security.

### **What I do to protect my information?**

As a best practice, we encourage individuals to remain vigilant against incidents of identity theft and fraud by reviewing their accounts and credit reports for suspicious activity, and to report any suspicious activity to the affiliated institutions immediately. As an added precaution, individuals can also review the steps you can take to protect against the possibility of identity theft and fraud below.

### **For more information.**

If you have questions, or need assistance, please call 844-558-4595, Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time, excluding major U.S. holidays. You may also write to the County at 109 South 3rd Avenue, P.O Box 449, Dillon, SC 29536.

### **Steps you can take to protect your information.**

All individuals are encouraged to remain vigilant against incidents of identity theft and fraud by reviewing their account statements and monitoring their free credit reports for suspicious activity and to detect errors. As a best practice individuals should frequently change their password for all online accounts. Under U.S. law, a consumer is entitled to one (1) free credit report annually from each of the three (3) major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit <http://www.annualcreditreport.com> or call, toll-free, 1 (877) 322-8228. Consumers may also directly contact the three (3) 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:

<b>Equifax</b>	<b>Experian</b>	<b>TransUnion</b>
<a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a>	<a href="https://www.experian.com/help/">https://www.experian.com/help/</a>	<a href="https://www.transunion.com/data-breach-help">https://www.transunion.com/data-breach-help</a>
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

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](http://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.