About the Accellion Cyberattack [1]

Cyberattack Update July 2, 2021

CU recently identified an additional set of files that were not included in the initial data review. Following a thorough review of this data, CU is now providing notice of this incident to those community members whose information was in these additional files. CU began notifying these individuals via mail or email beginning July 1, 2021.

Q. Why was this data not reviewed during the initial data review?
A. The Accellion system automatically destroys data after two weeks. There were files on the system that were stolen by the cyberattackers and then automatically purged before CU was informed by Accellion of the attack. When CU reviewed the Accellion files, some files had already been deleted and were inaccessible.

Q. How did CU find this additional data?
A. CU discovered the additional data when CLOP, the criminal organization tied to the cyberattack on Accellion, posted CU files on the dark web after not receiving a ransom payment. In March, CLOP posted a small amount of CU's data on the dark web and threatened to post more stolen data if CU did not pay a ransom. Based on guidance from the FBI, CU did not pay the cybercriminals. In mid-April, CU became aware that CLOP did post additional CU data on the dark web. CU downloaded and preliminarily reviewed these files and discovered the additional data that had been deleted from the Accellion system.

Q. Which campuses are affected?
A. The data in these additional files is related to the CU Boulder campus only. There was no additional data from CU Denver, Anschutz, or the Colorado Springs campuses.

Q. What is "Student Demographic Information"?
A. "Student Demographic Information" is limited to one or more of the following types of information: student's full name; home address; home telephone number; personal e-mail address; parent/guardian's name; place of birth; and/or their race/ethnicity.

Q. When I was a student at CU, my student id number was my social security number. If my student id was compromised, does that mean my social security number was compromised?
A. No, Student ID Number is not the same as Social Security Number. Although CU did use Social Security Numbers as Student ID Numbers in the past, this practice was discontinued and existing Student ID Numbers that were also Social Security Numbers were replaced with a new CU-generated Student ID Number.

Cyberattack Update April 21, 2021

Q: What “Student Financial Information” was impacted?
A: “Student Financial Information” does NOT include Financial Account Numbers, Payment Card Information, or Social Security Numbers. Nor does it include any banking information. Your letter will explicitly state if those data elements were exposed. In most cases, Student Financial Information included the amount of tuition paid for a semester, the date of payment, and whether or not the tuition was paid or partially paid by scholarship or grant. If you were a CU Boulder applicant, Student Financial Information may also include the range of family income that you provided in your CU Boulder application. We do not have reason to believe that the Student Financial Information is reasonably likely to be misused and we are providing the identity monitoring services out of an abundance of caution.

Q: What “Demographic Information” was impacted?
A: This information typically includes contact information, such as name, home address, phone number, email, parent/guardian names, gender, place of birth and/or race/ethnicity.

Q: Is this legitimate?
A: Yes. CU takes the security of information and its legal obligations very seriously. CU has provided notification to affected individuals through direct mailing or email as required by law. Two forms of notification letters were sent, based on the availability of contact information. Both forms state “LEGAL NOTICE OF DATA BREACH” at the top of the letter. The physical letters will arrive in an envelope with a clear window and the CU logo, sent from Fullerton, CA. The emailed letters are from “Dan Jones, Chief Information Security Officer” and have the subject line: “Notice of Data Breach.”

Q: I'm a faculty member and received a letter that says my Student ID was exposed, though I've never been a student at CU.
A: All faculty are assigned a Student ID number to associate them as the instructor of record in CU-SIS. This is a number for internal use only and Colorado statute requires notification following the exposure of these numbers.

Q: I've used the Large File Transfer service in the past. Is it possible my data was affected?
A: Individuals who sent files during the affected time window in January 2021 were promptly notified. If you did not receive the notifications from UCB OIT in January, the files you sent were not affected.

Q: What should I do if I receive a communication asking for ransom?
A: We recommend that you do not engage in any communication with the cybercriminals. If you receive an email, do not engage and delete the email. If the cybercriminals attempt to contact you by phone, hang up. If the cybercriminals attempt to contact you through text messages or through direct messages on social media (e.g. Facebook, Instagram, etc.), delete the message.

Cyberattack Update April 9, 2021

The University of Colorado Office of Information Security has largely completed its investigation into the late January cyberattack on CU's third-party vendor, Accellion. CU was one of at least 10 higher education institutions affected, in addition to several other Accellion corporate clients. All told, about 50 organizations were impacted. CU shut down the large file transfer service that was compromised immediately upon learning of the attack and has since migrated its large-file transfer platform to a different tool.

Frequently Asked Questions

Q: How many individual records were impacted?
A: Over 300,000 unique records with personal identifiable information (PII) were involved, most on the Boulder campus and some on the Denver campus.

Q: What is considered personal identifiable information?
A: PII can include social security numbers; personal identification numbers; passwords; pass codes; official state or government-issued driver's license or identification card numbers; government passport numbers; biometric data; employer, student, or military identification numbers; and financial transaction devices, including financial account numbers.

PII is defined in Colorado state statute, but it is important to note that CU is notifying individuals based on a broader definition. For example, the state definition for PII does not include demographic information, but we are taking a broader/more inclusive approach and will provide notification for this type of information as well.

Q: What specific types of information were compromised?
A: Information includes grades and transcript data, student ID numbers, race/ethnicity, veteran status, visa status, disability status, and limited donor information. It also includes some medical treatment information, diagnosis and prescription information.

Q: Is my Social Security number or bank account information at risk?
A: A small amount of social security numbers were involved.

Q: How will I know if my information is involved?
A: CU will send an email or regular mail notification to affected individuals on or after April 14.

Q: What is CU doing for those affected?
A: Qualifying individuals who have a social security number and a U.S. address will be provided credit monitoring, identity monitoring, fraud consultation and identity theft restoration.

Q: Who is paying for monitoring services and what is the cost?
A: Credit monitoring and identity monitoring services will be coordinated through University Risk Management. It will be provided at no cost to those impacted.

Q: What is the risk of identity theft?
A: While individuals should always be vigilant about the potential for identity theft, most of the information compromised in this attack would not easily lead to identity theft. Still, people should take appropriate precautions listed on this page and in notifications.

Q: Which campuses were affected? (*Updated 4/21/2021*)
A: Most of the impacted data was related to the Boulder campus, with an amount from the Denver campus. CU Colorado Springs and the CU Anschutz Medical Campus files were not affected. Individuals with a previous affiliation to either Boulder or Denver may have been affected, regardless of current affiliation.

Q: What steps can I take to protect my identity?
A: In addition to the resources you will receive in the notification, you can take steps below.

Q: How do I place a Fraud Alert on my account?
A: You may contact one of the major credit reporting companies for assistance. An **initial 90-day security alert** indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied.

Equifax Security Freeze	Experian Security Freeze	TransUnion (FVAD)
PO Box 105788	PO Box 9554	PO Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
1-800-685-1111	1-888-397-3742	1-800-888-4213
www.equifax.com [2]	www.experian.com [3]	www.transunion.com [4]

Q: How do I place a Security Freeze on my account?
A: This process is completed through each of the credit reporting agencies.

Equifax Security Freeze	Experian Security Freeze	TransUnion (FVAD)
PO Box 105788	PO Box 9554	PO Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
1-800-685-1111	1-888-397-3742	1-800-888-4213
www.equifax.com [2]	www.experian.com [3]	www.transunion.com [4]

Additional information:

Placing a freeze on your credit report will prevent lenders and others from accessing your credit report in connection with any new credit application, which will prevent them from extending credit. A security freeze generally does not apply to circumstances in which you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. With a security freeze in place, you will be required to take special steps

when you wish to apply for any type of credit. You should be aware that using a security freeze to take control over 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 or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report.

Q: What is the difference between a 'Fraud Alert' and a 'Security Freeze'?
A: A fraud alert notifies anyone requesting your credit file that you suspect you are a victim of fraud. As such, the lender should take steps to verify that you have authorized the request and deny any request that cannot be verified.

A security freeze will prevent lenders and others from accessing your credit report completely.

Q: What steps is CU taking to ensure this doesn't happen again?
A: Although the attack was on a vulnerability in software from a third-party vendor with which CU contracts, the university's Office of Information Security is conducting a lessons-learned exercise to improve processes and practices.

Q: Are the cybercriminals extorting CU?
A: Those responsible for the cyberattack have made extortion demands of CU and other Accellion clients.

Q: What are they demanding?
A: They want CU and/or individuals to pay ransom to prevent information from being posted to the dark web.

Q: Will CU pay the ransom?
A: On advice of the FBI (which is investigating the cyberattack) CU will not pay ransom.

Q: Why won't CU pay? Why shouldn't I?
A: There is no guarantee that the cybercriminals will honor promises to not post information. Nor is there assurance that they won't try further extortion.

Q: What should I do if I receive a communication asking for ransom?
A: Do not engage and delete the email.

CU uses a product called File Transfer Appliance (FTA) from Accellion to provide a large file transfer service used primarily by faculty, staff and researchers. The service is used primarily by the Boulder campus, although some data from the Denver campus was involved as well. System and campus information security teams are working to determine the extent of the attack and the precise nature of the data affected. This page provides information about the incident, what you can do to protect your data and the university's next steps.

The information below on this page was last updated: Friday, Feb. 12, 2021.

About the cyberattack
Accellion discovered an attacker was taking advantage of a vulnerability in its large file transfer software (FTA) and notified its clients. CU Boulder's Office of Information Technology (OIT) suspended use of the service [5] on Jan. 25, 2021 and issued a notice to users. The

service was restored on Jan. 28, 2021, after a patch was made available by Accellion and files and workspaces were successfully transferred to a new virtual appliance with the newly released version of the software.

A forensic investigation, led by the university's Office of Information Security (OIS) with the assistance of Accellion, revealed CU Boulder's service was compromised and the files available on the system during the attack had been at risk of unauthorized access.

What the University of Colorado is doing
On Monday, Feb. 1, 2021, OIT emailed the 447 CU users that had files uploaded in the large file transfer system in January. As part of the forensic investigation, users were asked to contact the Office of Information Security if they shared highly confidential data during the January timeframe.

OIS continues to conduct a manual review of all files that were exposed to unauthorized access. While the team is continually working on this, manual review can take some time. While we will have a sense of the extent of the attack by the end of this week, a complete investigation will take longer. The goal of this systematic and diligent review is to identify the types of data in these files so that we may work with all affected parties on next steps. Updates will be provided on this page as more details are confirmed regarding exposed data and affected parties.

What kind of data were compromised
While the full scope has not yet been determined, early information from the forensic investigation confirms that the vulnerability was exploited and multiple data types may have been accessed, including CU Boulder and CU Denver student personally identifiable information, prospective student personally identifiable information, employee personally identifiable information, limited health and clinical data, and study and research data.

At this point, data from CU Anschutz, UCCS and system administration does not appear to have been compromised, but the analysis is ongoing.

The results of the forensic investigation will provide information on the exposed data and allow us to provide affected parties with appropriate notification and offer remedies, where necessary.

What to do if you are concerned you are affected
All affected individuals will be notified in a timely manner as the investigation proceeds. Due to the nature of this service and its primary use by CU data custodians, individuals are unlikely at this time to know whether their personal data were impacted. To take proactive steps to protect your identity, learn more about actions you can take at https://www.identitytheft.gov/databreach [6].

Monitoring services will be made available at no cost for individuals whose confidentiality was compromised. These services detect identity fraud and credit fraud, along with restoration services to address any issues that arise. More information about these services will be provided in the notification letters sent to affected individuals.

Some additional resources to help protect yourself:

Fraud Alerts

- https://www.equifax.com/personal/ [7]
- https://www.transunion.com [8]
- https://www.experian.com/ [9]

You may place a fraud alert in your file by contacting one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freezes

You have the ability to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies. The credit reporting agencies may charge a fee to place a freeze, temporarily lift it or permanently remove it. The fee is waived if you are a victim of identity theft and have submitted a valid investigative or law enforcement report or complaint relating to the identity theft incident to the credit reporting agencies. You must review your state's requirement(s) and/or credit bureau requirement(s) for the specific document(s) to be submitted.

Other Resources

- Information about handling potential identity theft [10].

Other information

About Accellion File Transfer Appliance

The Large File Transfer service provided by OIT uses a software from Accellion called the FTA, or File Transfer Appliance. It is a solution OIT put in place to provide a mechanism for university faculty and staff to share large files, in lieu of sending them over email. It also provides a secure mechanism for sharing files, meeting the requirements for safe sharing of data required by HIPAA and FERPA. More benefits can be found here: https://oit.colorado.edu/services/file-transfer-storage-infrastructure/large-file-transfer [11]

Upcoming changes to file sharing
OIT is accelerating plans to move to a different file sharing product, which was not affected by this vulnerability. Two additional projects are underway to provide more robust file sharing and account security options for campus. One will migrate on-premises data to hosted cloud solutions and another will deliver a campus-supported multi-factor authentication solution.

Law enforcement and regulatory agencies
Pertinent law enforcement organizations (including the FBI) and appropriate state and federal regulatory agencies have been notified based on the information we have at this time.

Right Sidebar:
accellion_contact-info
Sub Title:

The University of Colorado experienced a cyberattack on a vulnerability in software provided by third-party vendor Accellion, which alerted the university in late January. CU is one of many Accellion customers that were affected by the attack. We believe personally identifiable information from students, employees and others may have been compromised. <hr>

Source URL:https://www.cu.edu/accellion-cyberattack

Links
[1] https://www.cu.edu/accellion-cyberattack [2] http://www.equifax.com [3] http://www.experian.com
[4] http://www.transunion.com [5] https://oit.colorado.edu/node/26376
[6] https://www.identitytheft.gov/databreach [7] https://www.equifax.com/personal/
[8] https://www.transunion.com/ [9] https://www.experian.com/ [10] https://www.cu.edu/security/worried-about-identity-theft [11] https://oit.colorado.edu/services/file-transfer-storage-infrastructure/large-file-transfer