PERKINSCOIE

1201 Third Avenue
Suite 4900
Seattle, WA 98101-3099

T +1.206.359.8000
F +1.206.359.9000
PerkinsCoie.com

May 28, 2021

Amelia M. Gerlicher
AGerlicher@perkinscoie.com
D. +1.206.359.3445
F. +1.206.359.4445

VIA EMAIL (attorneygeneral@doj.nh.gov)

State of New Hampshire
Department of Justice
Office of the Attorney General Gordon J. MacDonald
33 Capitol Street
Concord, NH 03301

Re: Notification of Security Incident

Dear Mr. MacDonald:

We write on behalf of our client, the Stanford University School of Medicine. Stanford used a third-party file-sharing service, called File Transfer Appliance, provided by Accellion, Inc. (the "Accellion FTA"). As reported in the media, Accellion discovered a vulnerability in January 2021 that permitted bad actors to bypass the FTA's encryption and illegally gain access to files temporarily stored on Accellion FTA devices.

After Accellion notified Stanford of the software vulnerability, Stanford immediately took its Accellion FTA offline and launched an investigation to determine whether it had been a victim of this cyberattack.

The investigation identified evidence of suspicious activity targeting Stanford's Accellion FTA on January 21, 2021, but it was not clear at that time whether files had been exfiltrated, and if so, whether those files contained personally identifiable information. On March 29, 2021, certain files from the Stanford Accellion FTA were made available online by unknown individuals. At that time, Stanford had no reason to believe that information regarding residents of your state had been affected. However, on April 23, 2021, Stanford discovered that one file affected in the incident contained data including personal information of 4 residents of your state.

Stanford notified law enforcement and is continuing to investigate this incident. It has permanently discontinued use of the Accellion FTA.

Stanford is an Affiliated Covered Entity under the Health Insurance Portability and Accountability Act of 1996, as amended. It is sending the enclosed notification pursuant to 45 C.F.R § 164.404 beginning May 28, 2021.

Very truly yours,

Amelia M. Gerlicher

Stanford School of Medicine
C/O IDX
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<XXXXXXXX>>

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

May 28, 2021

RE: Notice of Security Incident

Dear <<First Name>> <<Last Name>>,

We are writing to inform you that some of your personal information was involved in a recent data security incident that affected a third-party software product used by the Stanford School of Medicine.

What Happened

The Stanford School of Medicine used a third-party file sharing product, provided by a company called Accellion, to securely transfer electronic information. A flaw in Accellion's software was used by bad actors to illegally gain access to some files stored on the system.

The attack on Accellion's product affected many organizations across the country, including other universities, health care centers, and companies. After Accellion told Stanford of the software vulnerability, Stanford immediately stopped using the product and launched an investigation to determine if it had been a victim of this cyberattack.

The investigation identified evidence of suspicious activity targeting the Accellion product on January 21, 2021, but it was not clear at that time which files had been stolen. On March 29, 2021, certain files from the Stanford School of Medicine's Accellion system, which we now know included your information, were made available online by unknown individuals. The investigation into the incident is still in progress, and we have notified law enforcement, including the Federal Bureau of Investigation (FBI), which is also investigating the cyberattack by the bad actors.

What Information Was Involved

Documents taken in the attack included [redacted]

What We Are Doing

We are offering you the option, at no cost to you, to enroll in identity theft protection services through IDX (a company that provides those services). These services include <<12/24>> months of credit and CyberScan monitoring, an insurance reimbursement policy, and fully managed ID theft recovery services. If you'd like to activate this coverage, please visit https://app.idx.us/account-creation/protect or call 1-800-939-4170 and use the Enrollment Code above. IDX representatives are available Monday through Friday from 6 am to 6 pm Pacific Time. Please note the deadline to enroll is August 28, 2021.

What You Can Do, and More Information

Other entities involved in the Accellion attack have reported that the attackers have sent emails attempting to scare people into giving them money. Please forward any such email to privacy@stanford.edu or simply delete it. We recommend that you do not respond.

In addition to enrolling in credit monitoring as described above, we recommend the following steps to monitor for potential misuse of your personal information:

- You should regularly review your account statements and monitor free credit reports.

- Under federal law, you are entitled to obtain one free copy of your credit report every twelve months from each of the nationwide consumer reporting agencies. You can obtain a free copy of your credit report from each agency by calling 1-877-322-8228 or by visiting www.annualcreditreport.com. We recommend that you periodically obtain credit reports from each nationwide credit reporting agency. If you discover information on your credit report arising from a fraudulent transaction, you may request that the credit reporting agency delete that information from your credit report file.

- You may also consider contacting the credit reporting agencies directly if you wish to put in place a fraud alert or a security freeze. A fraud alert will notify any merchant checking your credit history that you may be the victim of identity theft and that the merchant should take additional measures to verify the application. Contacting any one of the three agencies will place an alert on your file at all three. A security freeze restricts all creditor access to your account but might also delay any requests you might make for new accounts.

    - Equifax: 800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241
    - Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9554, Allen, TX 75013
    - TransUnion: 800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

- You can also find additional steps to take, and report incidents of identity theft, at the Federal Trade Commission's website at https://identitytheft.gov.

Please know that we take the privacy and security of your information seriously. We deeply regret any worry or inconvenience that this criminal act may cause you. If there is anything else that we can do to assist you, or if you have any questions or concerns regarding this matter or your information affected, please feel free to contact 1-800-939-4170.

Sincerely,

Michael Tran Duff
Chief Information Security Officer and Chief Privacy Officer
Stanford | University Privacy Office

IMPORTANT CONTACT INFORMATION

You may obtain information about avoiding identity theft from the FTC. The FTC can be reached at:

Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20850
www.consumer.gov/idtheft, 1-877-ID-THEFT (1-877-438-4338)

IF YOU ARE A MARYLAND RESIDENT: You may also obtain information about avoiding identity theft from the Maryland Attorney General's Office. This office can be reached at:

Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202
www.oag.state.md.us, (888) 743-0023

IF YOU ARE A NORTH CAROLINA RESIDENT: You may also obtain information about preventing identity theft from the North Carolina Attorney General's Office. This office can be reached at:

North Carolina Department of Justice, 9001 Mail Service Center, Raleigh, NC 27699-9001
www.ncdoj.com, (877) 566-7226

IF YOU ARE AN RHODE ISLAND RESIDENT: You may obtain information about preventing identity theft from the Rhode Island Attorney General's Office. This office can be reached at:

Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903
www.riag.ri.gov, (401) 274-4400

IF YOU ARE A NEW YORK RESIDENT: You may also obtain information about preventing identity theft from the New York Department of State's Division of Consumer Protection. This office can be reached at:
New York State Division of Consumer Protection
123 William Street, New York, NY 10038-3804
One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001
www.dos.ny.gov/consumerprotection, 1 (800) 697-1220

IF YOU ARE A DISTRICT OF COLUMBIA RESIDENT: You may also obtain information about preventing identity theft from the D.C. Attorney General's Office. This office can be reached at:

Office of Consumer Protection, 441 4th Street, NW, Washington, DC 20001
oag.dc.gov/consumer-protection, (202) 442-9828