



Donna B. Maddux
888 SW Fifth Avenue, Suite 900
Portland, OR 97204
Donna.Maddux@lewisbrisbois.com
Direct: (971) 334-7001

February 15, 2021

VIA ELECTRONIC SUBMISSION

Attorney General Brian Frosh
Maryland Attorney General's Office
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
E-Mail: Idtheft@oag.state.md.us

Re: Notification of Data Security Incident

Dear Attorney General Frosh:

Lewis Brisbois Bisgaard & Smith LLP represents Linical Accelovance America, Inc. ("Linical Americas") in connection with a recent data security incident that may have affected the information of certain Maryland residents. The purpose of this letter is to notify you of the incident in accordance with Maryland's data breach notification statute.

1. Nature of the data security incident.

Linical Americas is the U.S. subsidiary of Linical Co. LTD, a multinational clinical research organization specializing in supporting clients in their development of therapeutic agents for human use. Linical America's parent company is headquartered in Japan and has an affiliate network operating in the Americas, Europe, China, Korea, and Taiwan. Linical Americas' current headquarters are in Stuart, Florida, and its previous headquarters were in Rockville, Maryland.

In October 2021, Linical Americas was notified that two operational regions (Europe and Japan) under its parent company were victims of ransomware attacks. Upon discovering this activity, Linical's operations worldwide immediately took steps to further secure the digital environment. Linical's impacted regions engaged leading cybersecurity firms to assist with investigations to determine whether personal information may have been impacted as a result of the incident. These investigations revealed that an unauthorized actor gained access to and obtained certain data from the Linical networks in Europe and Japan.

Linical undertook a comprehensive review of the information that could have been accessed and acquired as a result of the incident. On January 24, 2022, Linical determined that personal information,

primarily related to its employees, was impacted. The information potentially accessed without authorization may have included first and last name, along with their Social Security number.

2. Number of Maryland residents affected.

Linical determined that thirty-five (35) Maryland residents were impacted in this incident. Notification letters were mailed to all affected individuals on February 15, 2022. A sample copy of the letter provided to impacted individuals is included with this letter.

3. Steps taken relating to the incident.

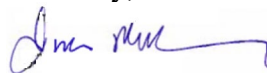
Linical has taken significant affirmative steps to help minimize the risk of a similar situation arising in the future and to protect the privacy and security of all personal information in its possession. These steps have included working with software development experts to implement a number of security measures to better protect their digital environment.

While Linical Americas has no indication that the information has been misused, it nonetheless is providing individuals with information about steps that they can take to help protect their personal information. As a further precaution, Linical Americas is also offering Maryland consumers one (1) year of complimentary credit and identity monitoring services through Kroll. This product helps detect possible misuse of personal information and provides consumers whose information may have been accessed without authorization with identity protection support.

4. Contact information.

Linical Americas is committed to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact me at (971) 334-7001, or by e-mail at Donna.Maddux@lewisbrisbois.com.

Sincerely,



Donna B. Maddux of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<b2b_text_1(C/O name)>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Re: Notice of Potential Data Security Incident

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

Linical Accelovance America, Inc. (“Linical Americas”) is writing to inform you of a recent data security incident that may have involved some of your personal information. At Linical Americas, we take the privacy and security of all information within our possession very seriously. That is why we are writing to provide you with information about this incident, about steps you can take to help protect your personal information, and to offer you complimentary credit and identity monitoring services.

What Happened? In October 2021, Linical Americas was notified that two operational regions (Europe and Japan) under its parent company, Linical Co. LTD, were victims of cybersecurity attacks. Upon discovering this activity, Linical’s operations worldwide immediately took steps to further secure the digital environment. Linical’s impacted regions engaged leading cybersecurity firms to assist with investigations to determine whether personal information may have been impacted as a result of the incident. These investigations revealed that an unauthorized actor gained access to and obtained certain data from the Linical networks in Europe and Japan. On January 24, 2021, we determined that some of your personal information may have been involved this incident. We have no reason to believe that your personal information has been misused as a result of this incident.

What Information Was Involved? The information potentially impacted is any information you provided to Linical Americas and may include your name and Social Security number.

What We Are Doing: As soon as the incident was discovered, Linical took the steps referenced above and implemented additional security features to reduce the risk of a similar incident occurring in the future. We are further notifying you of this event and advising you about steps you can take to help protect your information. In addition, out of an abundance of caution, we are offering you complimentary credit and identity monitoring services for 12 months through Kroll, a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data.

Kroll’s services include 12 months of Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration. With these services, Kroll will help you resolve issues if your identity is compromised.

What You Can Do: Please review this letter carefully, along with the guidance included with this letter about additional steps you can take to help protect your information. You can also activate Kroll’s identity monitoring services, which are offered to you at no cost.

How to Activate:

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

To receive identity monitoring services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file. For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

If you prefer to activate these services offline and receive monitoring alerts via the US Postal Service, you may activate via our automated phone system by calling 1-888-653-0511, Monday through Friday, 8:00 a.m. to 5:30 p.m. Central time, excluding major U.S. holiday. Please have your membership number located in your letter ready when calling. Please note that to activate monitoring services, you will be required to provide your name, date of birth, and Social Security number through our automated phone system. Additional information describing your services is included with this letter.

Kroll representatives are available by calling 1-???-???-???? Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please note the deadline to activate is <<b2b_text_6(activation deadline)>>. Please do not discard this letter, as you will need the Membership Number provided above to access services.

Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Vita M. Lanoce", with a long horizontal flourish extending to the right.

Vita M. Lanoce, MS
Chief Executive Officer
Linical Accelovance America, Inc.

ADDITIONAL STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC). You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.consumer.ftc.gov, www.ftc.gov/idtheft.

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285, www.equifax.com.
- *Experian*, P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com.
- *TransUnion*, P.O. Box 1000, Chester, PA 19016, 1-800-916-8800, www.transunion.com.

Fraud Alerts: There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary proof. An extended fraud alert is also free and will stay on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>. Military members may also place an Active Duty Military Fraud Alert on their credit reports while deployed. An Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment.

Credit or Security Freezes: Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit.

You must separately place a security freeze on your credit file with each credit reporting agency. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the Federal Trade Commission identified above. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after receiving your request.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state attorney general about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the attorney general in your state.

Additional information:

District of Columbia: The Office of the Attorney General for the District of Columbia can be reached at 400 6th Street, NW, Washington, DC 20001; (202) 727-3400; oag@dc.gov.

Maryland: Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 1-888-743-0023; oag@state.md.us or IDTheft@oag.state.md.us.

North Carolina: North Carolina Attorney General's Office, Consumer Protection Division, can be reached at: 9001 Mail Service Center Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.

New York: New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005, 1-212-416-8433, <https://ag.ny.gov/>.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.