GIBSON DUNN

Stephenie Gosnell Handler
Partner
T: +1 202.734.8920
shandler@gibsondunn.com

April 1, 2026

VIA EMAIL
Consumer Protection & Antitrust Bureau
Office of the Attorney General
New Hampshire Department of Justice
1 Granite Place South
Concord, NH 03301
DOJ-CPB@doj.nh.gov

To Whom It May Concern:

We are writing on behalf of Synopsys, Inc. ("Synopsys") to provide notice regarding a cybersecurity incident that involves the personal information of a New Hampshire resident.

On December 3, 2025, Synopsys identified unauthorized activity. Upon detection, Synopsys's incident response team immediately investigated, supported by leading cybersecurity experts. To date, the investigation has determined that a small number of Synopsys email accounts were subject to unauthorized access between June 17, 2025 and December 4, 2025. The incident has been contained. The affected information varied by individual, but may have included: first and last name, social security number, driver's license number and/or other government identification number, date of birth, address, email address, bank account number and/or other financial information, and/or medical or health insurance information.

We are taking steps designed to enhance the security of our systems and to help prevent recurrence.

In connection with this incident, we are offering the New Hampshire resident that is being notified a complimentary 24-month membership of Equifax Credit Watch™ Gold.

In an effort to promptly notify affected residents about this incident, starting today we will be sending a notice to the impacted New Hampshire resident via U.S. First Class Mail in the form attached as **Exhibit A**.

If you have any questions, I can be reached by email at Shandler@gibsondunn.com or directly by telephone at (202) 734-8920.

Thank you for your attention to this matter.

Sincerely,

S. Handler

Stephenie Gosnell Handler
GIBSON, DUNN & CRUTCHER LLP

Exhibit A

Synopsys, Inc.
675 Almanor Ave
Sunnyvale, CA 94085
T 650-584-5000

April 1, 2026

00695-ADFFIN L001 AUTO *000002
MT263V5041
000002

Sample Recipient
123 Elm St Apt 2
Anytown AZ 85212

NOTICE OF DATA BREACH

Dear Sample Recipient,

At Synopsys, Inc., we take the security of your personal information very seriously. We are writing to let you know about a recent cybersecurity incident that impacted some of your personal information. We are contacting you to explain the circumstances of the incident, the types of information involved, and steps you can take.

What happened? On December 3, 2025, Synopsys identified unauthorized activity by a malicious third party. We immediately launched an investigation, supported by leading cybersecurity experts. To date, the investigation has determined that a small number Synopsys email accounts were subject to unauthorized access by the malicious third party between June 17, 2025 and December 4, 2025, including emails that may have contained some of your personal information.

What information was involved? The affected information varied by individual, but may have included: first and last name, social security number, driver's license number and/or other government identification number, date of birth, address, email address, bank account number and/or other financial information, and/or medical or health insurance information.

What are we doing? We have conducted a robust investigation with the support of leading cybersecurity experts, and have confirmed the incident has been contained. We have also taken steps designed to enhance our network security and help prevent recurrence, and we are regularly reviewing and updating such security measures.

As a precaution, we are offering you complementary credit monitoring, identity theft detection and resolution services described in Attachment A.

What can you do? We recommend you review the enclosed Information About Identity Theft Protection, and encourage you to stay vigilant for incidents of fraud and identify theft. We also recommend that you continue to review your financial accounts, account statements, and free credit reports for any suspicious activity.

For more information: We sincerely regret this incident happened. If you have any questions or concerns, please contact 1-844-558-4664.

Yours sincerely,

Synopsys, Inc.

00695-ADFFIN-218098-L001 AUTO_000002-000005-000-1/2

MT263V5041

ATTACHMENT A
Instructions for Activating Equifax Credit Watch™ Gold

Sample Recipient
Enter your Activation Code: **123456789012**
Enrollment Deadline: **August 31, 2026**

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4]

Enrollment Instructions

Go to ***www.equifax.com/activate***

Enter your unique Activation Code of **123456789012** then click "Submit"

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout**:
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

You're done!
The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

[1]WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded. [2]The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC. [3]Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com [4]The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Information about Identity Theft Protection

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228 or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC's") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three nationwide consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, please review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so 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 consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information cannot be explained, then you will need to call the creditors involved. Information that cannot be explained also should be reported to law enforcement because it may signal criminal activity. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. This notice has not been delayed by law enforcement.

Report Incidents. If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. For more information, please visit https://www.identitytheft.gov/.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

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

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. 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, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax	**Experian**	**TransUnion**
Equifax Information Services LLC	Experian Inc.	TransUnion LLC
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19016
1-888-836-6351	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Consider Placing a Security Freeze on Your Credit File. You may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually. There is no charge to place or lift a security freeze. For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

00695-ADFFIN-218098-L001 AUTO_000002-000007-000-2/2

MT263V5041

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

For Maryland Residents.
You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:
Maryland Office of the Attorney General, Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023 or (410) 576-6300
www.marylandattorneygeneral.gov

For Washington, D.C. Residents.
You may obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia at:
Office of the Attorney General for the District of Columbia
400 6th Street NW
Washington, D.C. 20001
(202) 727-3400
www.oag.dc.gov