

Jennifer L. Morris, Esq.
Dunlap Bennett & Ludwig
1200 G Street NW Suite 800
Washington, DC 20005
jmorris@dblawyers.com
202-327-3217

****Confidential Information Provided Voluntarily****

VIA US Mail

State of Maryland
Office of the Attorney General
200 ST. Paul Place, Baltimore, MD 21202

Re: Attorney General – Voluntary Notice of Third-Party Vendor Data Breach

To Whom It May Concern:

Our firm was retained to provide support and compliance notification with regards to U.S.-based businesses and customers whose data may have been compromised as a result of a third-party vendor's data breach. This letter provides voluntary notification on behalf of CMT Industrial Solutions, LLC ("Company") of a recent data breach involving a third-party e-commerce platform that residents of Maryland used to purchase Company's products.

SignatureIT Ltd. (an Israeli-based company with U.S. subsidiaries) is a third-party that owns and operates e-commerce platforms that are often used by Company's customers to purchase Company products. SignatureIT recently notified Company of unauthorized access and interruption of these platforms. The data and systems (including Enterprise Resource Platform) owned and operated by Company are not a part of the e-commerce platforms and are completely separate and secure.

Even though there was no unauthorized access of Company systems, Company acted with caution and notified all known U.S. users registered with the e-commerce platform on or before November 16, 2023, of the third-party data breach to ensure each individual could take action to protect their information. This notice was provided electronically to said users on or about December 6, 2023. At the time of this notice, Company believes that approximately 3 residents may have had their personal information compromised as a result of the SignatureIT data breach. For your convenience, we have enclosed a copy of the Notice of Third-Party Data Breach that was sent to residents, without including any Personally Identifiable Information.

What Happened?

On or about November 16, 2023, SignatureIT noticed unusual activity on their network, including a suspicious email sent to a multitude of users of its e-commerce platforms. According to a forensic preliminary report obtained by SignatureIT and subsequently shared, in part, with Company and/or its affiliates, the experts identified the Confluence collaboration platform as the probable penetration point into SignatureIT's system. Consequently, SignatureIT's e-commerce platforms were shut down.

What Information Was Involved?

Personal information entered when subscribing to, or using, SignatureIT's e-commerce platforms may have been accessed by an unauthorized third-party. Potential categories of information that purchasers may have entered into

the SignatureIT e-commerce platforms include: (i) First and Last name, (ii) Shipping Address, (iii) Billing Address, (iii) Phone and Facsimile numbers, (iv) Company Names, (vi) VAT Numbers, (vii) Titles, (viii) ERP Account numbers, (ix) Passwords to access the Signature IT Account, (x) Shipping Methods, (xi) Courier collect numbers and delivery types, (xii) Payment terms, (xiii) Tax-free status, (xiv) Currencies, (xv) Positions, or (xvi) Transaction details (quantities, products ordered).

Since all information was stored on SignatureIT servers, Company does not have the precise scope or content of the data that was accessed.

What is the Company Doing?

As a precautionary measure, notifications were sent to relevant regulators. These include the U.S. Federal Bureau of Investigation and to the Cybersecurity and Infrastructure Security Agency under the Cyber Incident Reporting for Critical Infrastructure Act, applicable U.S. state agencies, and the E.U. under the General Data Protection Regulation. Company has also notified the nationwide consumer reporting agencies. Although data stored in Company information systems was not accessed, and even though Company was not directly involved in this incident, Company continues to monitor this incident and its effect on its customer community.

If you have any further questions or need additional information, please feel free to contact me at jmorris@dbllawyers.com.

Sincerely,

/s/JLM

Jennifer L. Morris
Partner

Encl. Copy of Third-Party Data Breach Notification Letter



MORE THAN A SOURCE — A RESOURCE.

RE: NOTICE OF THIRD-PARTY DATA BREACH

Dear Customer:

We write to notify you of a potential data-breach incident, involving a third-party e-commerce platform that you used in order to facilitate ordering our products. SignatureIT Ltd., a third party who owns and operates the said e-commerce platform, recently notified us of unauthorized access and interruption of this platform.

Our data and systems (including ERP) are not a part of this e-commerce platform and are completely separate. Therefore, please be reassured that, in line with the opinion of cyber experts who investigated the matter, these (our) systems remained fully secured and were unaffected by the event.

What Happened?

On November 16, 2023, SignatureIT noticed unusual activity on their network, including a suspicious email sent to a multitude of users of its e-commerce platforms.

According to a forensic preliminary report that was obtained by SignatureIT, the experts identified the Confluence collaboration platform as the probable penetration point into SignatureIT's system. Consequently, SignatureIT's e-commerce platforms were shut down. Accordingly, SignatureIT notified us on or about November 16, 2023, that its e-commerce platforms suffered a data breach.

Since all of the information was stored on SignatureIT servers, we do not have the precise scope or content of the data that was accessed. Therefore, out of an abundance of caution, we are notifying all users who were registered until November 16, 2023, as authorized to use the e-commerce platform.

What Information Was Involved?

Personal information entered when subscribing for, or using, SignatureIT's e-commerce platform may have been accessed by an unauthorized third party. Potential categories of information you may have entered into the SignatureIT e-commerce platform and which may have been accessed include: (i) First and Last name, (ii) Shipping Address, (iii) Billing Address, (iii) Phone and Facsimile numbers, (iv) Company Names, (vi) VAT Numbers, (vii) Titles, (viii) ERP Account numbers, (ix) Passwords to access the Signature IT Account, (x) Shipping Methods, (xi) Carrier collect numbers and delivery types, (xii) Payment terms, (xiii) Tax-free status, (xiv) Currencies, (xv) Positions, or (xvi) Transaction details (quantities, products ordered).

What Are We Doing?

As a precautionary measure, notifications were sent to relevant regulators. These include the U.S. Federal Bureau of Investigation and to the Cybersecurity and Infrastructure Security Agency under the Cyber

300 Industrial Drive
Greenville, SC 29607

2223 Executive Street, Suite C
Charlotte, NC 28208

6402 Commonwealth Drive
Roanoke, VA 24018

WWW.CMTINDUSTRIAL.COM
(864) 271-2871

Incident Reporting for Critical Infrastructure Act, applicable U.S. state agencies, and the E.U. under the General Data Protection Regulation. Relevant information is still being gathered to ensure the security of our customers' information and we are working diligently to restore a secure e-commerce platform.

Although data stored in our information systems was not accessed, and even though we were not directly involved in this incident, we continue to monitor this incident and its effect on our customer community. To any extent needed, we will work with law enforcement agencies as may be needed in their investigation of the breach.

What Can You Do?

It is important to stay vigilant and protect yourself from the possibility of fraud and identity theft. We strongly recommend that you: 1) change your password for any account in which you used the same or similar password which you used for the SignatureIT e-commerce platform; 2) monitor your online accounts and review credit reports for suspicious activity, and report any suspected incident of identity theft to local law enforcement or your Attorney General's Office; 3) contact any of the three credit bureaus below in order to place a fraud alert on your accounts, should you have any concern that any of your personal information (including credit card and/or banking details) was/ were provided by you when using the e-commerce platform.

EXPERIAN	EQUIFAX	TRANSUNION
(toll-free) 888-397-3742 P.O. Box 4500 Allen, TX 75013 www.experian.com	(toll-free) 888-378-4392 P.O. Box 740241 Atlanta, GA 30374 www.equifax.com	(toll-free) 800-916-8800 P.O. Box 2000 Chester, PA 19022 www.transunion.com

You are entitled to a free credit report every year from each of these agencies at: www.annualcreditreport.com.

If you are employed with a U.S. Defense Contractor and/or support any U.S. Federal or State government contracts, we also recommend that you notify appropriate personnel within your company so they can assess whether this third-party cyber incident requires any reporting by your company in accordance with FAR 52.239-1, *Privacy or Security Safeguards*; DFARS 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*; and/or other federal law, regulation, or policy.

For More Information

If you need further assistance related to the reported incident, please reach out to your contact person with us, or call +1-864-271-2871, at or write us at 300 Industrial Drive, Greenville, SC 29607.

We are relieved that our systems were not impacted by this data incident and hope this third-party incident does not negatively impact you in any way.

Very truly yours,

Jason Dierks
Director of Operations

Enclosure: Information Regarding Identity Theft Protection