IceMiller
LEGAL COUNSEL

200 W. Madison | Suite 3500 | Chicago, IL 60606-3417

November 1, 2022

REENA R BAJOWALA
DIRECT NUMBER: 312-726-6220
DIRECT FAX: 312-726-6292
Reena Bajowala@icemiller com

CONFIDENTIAL

VIA ELECTRONIC MAIL (DOJ-CPB@DOJ.NH.GOV)

Attn: Notification of a Data Breach

Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Written Notification of a Data Breach

To Whom It May Concern:

On behalf of my client, Convergent Outsourcing, Inc. ("Convergent"), I am hereby submitting a written notification of a data breach, in compliance with N.H. Rev. Stat. §§ 359-C:19 et seq.

On June 17, 2022, Convergent discovered that an external actor gained unauthorized access to its systems and deployed a ransomware malware. The investigation also revealed that, also on June 17, 2022, the unauthorized actor deployed certain data extraction tools on a drive located at a remote branch of Convergent that is used to store and share files internally. The share drive was encrypted and corrupted by the unauthorized actor.

Upon discovery of the incident, Convergent engaged its internal experts and legal counsel to identify the scope of the incident. Convergent also notified law enforcement. Convergent immediately began taking steps to secure its systems and isolate its impacted servers against additional spread and sever the unauthorized actor's access to its networks and drives.

Convergent's review of the unauthorized actor's activities show that the actor was likely targeting Convergent data and servers in order to disrupt services and force ransom payment. The investigation did not reveal any misuse of personal information, or any attempts at fraud or identity theft.

Subsequent to this event, Convergent took immediate action to secure its systems and proactively manage its network. Convergent reset all passwords, and engaged third-party experts

to assist with containment, removal, and restoration. Convergent also coordinated with its clients and vendors to inform them of the incident to ensure that they deploy similar proactive measures and reviewed their policies and procedures relating to data privacy and security to further harden Convergent's systems against future attacks.

Nonetheless, out of an abundance of caution, we are notifying **2,045** New Hampshire residents. A copy of the notice that will be sent to the affected New Hampshire residents on October 26, 2022, is attached herewith. Credit monitoring and identity theft protection services will be offered to the affected New Hampshire residents for a period of twelve (12) months.

If you require further information about this matter, please contact me by telephone at (312) 726-6220 or via email at reena.bajowala@icemiller.com.

Sincerely,

ICE MILLER, LLP

Reena R. Bajowala

Attachment: Individual Notification Letter

To Enroll, Please Call:
1-833-814-1691
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code:
<<XXXXXXXX>>

<<Return Address>>
<<City>>, <<State>> <<Zip>>

<<FirstName>> <<MiddleInitial>> <<LastName>>
<<Addr1>> <<Addr2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

October 26, 2022

NOTICE OF DATA BREACH

Dear <<FirstName>> <<LastName>>:

Convergent Outsourcing, Inc. ("Convergent") is sending this letter as part of our commitment to privacy. Convergent performs debt collection services and, during the course of performing those services, receives personal information. We are contacting you regarding a security incident at Convergent which may have involved some of your personal information.[1] We want you to understand what happened, what we are doing about it, the steps you can take to protect yourself, and how we can help you.

What Happened.

On June 17, 2022, we became aware of an interruption to certain services performed by Convergent affecting certain computer systems. We immediately began taking steps to secure our

[1] Note, the security incident also impacted the business operations of Convergent's affiliate, Account Control Technology, Inc. ("ACT"). To the best of our knowledge, per our investigation, you are receiving this letter because your information was found in certain information held in connection with Convergent's operations.

systems and launched an investigation to better understand the nature of the service interruption. We immediately took action to secure our systems, isolated any impacted servers against additional spread and severed the unauthorized actor's access to our network and servers. We, with the assistance of third party experts, also expanded our investigation to search for and review any personal information on our systems that could have been accessed.

We discovered that an external actor gained unauthorized access to our systems and deployed a ransomware malware. The investigation also revealed that the unauthorized actor deployed certain data extraction tools on one storage drive that is used to save and share files internally.

What Information Was Involved.

Please note that we are providing this information in an abundance of caution, as the thorough investigation could not confirm your personal information was *actually* viewed by the unauthorized actor.

However, our investigation revealed the following personal information may have been involved in the unauthorized actor's access of the internal drive referenced above: name, contact information, financial account number, and social security number.

What We Are Doing.

Convergent takes the confidentiality, privacy, and security of information in our care seriously. When we discovered the service interruption, we, with the assistance of third party experts, immediately deployed an array of containment and remediation steps.

We immediately took action to secure our systems and proactively managed our network to sever connectivity and prevent the movement of the unauthorized actor. We reset all passwords, and engaged third-party experts to assist with containment, removal, and restoration. We also coordinated with our clients and vendors to inform them of this event so they could deploy similar proactive measures on their own computer systems. We have since deployed additional cybersecurity measures and reviewed policies and procedures relating to data privacy and security to further harden our systems against future attacks.

While the investigation has not revealed any misuse of your personal information, nor any attempts at fraud or identity theft, out of an abundance of caution, we are providing you with twelve months of credit monitoring and identity protection services through IDX at no cost to you. A description of the services and instructions on how to enroll can be found below in the *What You Can Do* section. Please note that you must complete the enrollment process yourself, as we are not permitted to enroll you in these services on your behalf.

What You Can Do.

While we are not aware of any misuse of your personal information, below is information about steps that an individual may take to protect against potential misuse of their personal information.

We encourage you to, as always, remain vigilant and monitor your account statements, insurance transactions, and free credit reports for potential fraud and identity theft, and promptly report any concerns. We also suggest you regularly review bills, notices, and statements. You should always be alert in monitoring account statements and transactions for fraud and identity theft, and promptly report any questionable or suspicious activity.

In addition, you may contact the Federal Trade Commission ("FTC") or law enforcement, including your state Attorney General, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's Web site, at www. ftc.gov/idtheft, or call the FTC, at (877) IDTHEFT (438-4338) or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You may also periodically obtain credit reports from each nationwide credit reporting agency. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. In addition, under the federal Fair Credit Reporting Act ("FCRA"), you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You may contact the nationwide credit reporting agencies at:

Equifax	Experian	TransUnion
(800) 685-1111	(888) 397-3742	(888) 909-8872
P.O. Box 740241	P.O. Box 9701	Fraud Victim Assistance Division
Atlanta, GA 30374-0241	Allen, TX 75013	P.O. Box 2000
www.Equifax.com/personal/credit-report-services	www.Experian.com/help	Chester, PA 19022
		www.TransUnion.com/credit-help

You also have other rights under the FCRA. For further information about your rights under the FCRA, please visit: http://files.consumerfinance.gov/f/201410_cfpb_summary_your-rights-under-fcra.pdf.

In addition, you may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file.

In addition, you can contact the nationwide credit reporting agencies at the phone numbers listed above to place a security freeze to restrict access to your credit report. There is no charge to place, lift or remove a security freeze. You will need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your request, each credit reporting agency will send you a confirmation letter containing a unique PIN or password that you

will need in order to lift or remove the freeze. You should keep the PIN or password in a safe place.

We also encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1- 833-814-1691 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. The deadline to enroll is January 26, 2023.

For More Information.

If you have questions about this letter, please call 1-833-814-1691 toll-free Monday through Friday from 9 am - 9 pm Eastern Time, or go to https://app.idx.us/account-creation/protect. The toll free number and website have been created to answer your questions about the incident and to help you enroll in identity theft and credit monitoring services.

We sincerely apologize for the worry and inconvenience this matter may cause. Convergent is committed to continued transparency and support for those potentially impacted by the incident.

Sincerely,

Convergent Outsourcing, Inc.

IF YOU ARE A DISTRICT OF COLUMBIA RESIDENT: You may obtain information about avoiding identity theft from the FTC or the District of Columbia Attorney General's Office. These offices can be reached at:

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

Office of the Attorney General
441 4th Street, NW
Suite 1100 South
Washington, DC 20001
(202) 727-3400
https://oag.dc.gov/

IF YOU ARE AN IOWA RESIDENT: You may obtain information about avoiding identity theft from the FTC or the Iowa Attorney General's Office. These offices can be reached at:

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

Office of the Attorney General of Iowa
Hoover State Office Building
1305 E. Walnut St
Des Moines, IA 50319
(515) 281-5164
https://www.iowaattorneygeneral.gov/

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

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

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

IF YOU ARE A NEW YORK RESIDENT: You may obtain information about security breach response and identity theft prevention and protection from the FTC or from the following New York state agencies:

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

New York Attorney General
Consumer Frauds &
Protection Bureau
120 Broadway, 3rd Floor
New York, NY 10271
(800) 771-7755
www.ag.ny.gov

New York Department of State
Division of Consumer Protection
99 Washington Avenue
Suite 650
Albany, New York 12231
(800) 697-1220
www.dos.ny.gov

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

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

North Carolina Department of Justice
Attorney General Josh Stein
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
http://www.ncdoj.com

IF YOU ARE AN OREGON RESIDENT: You may contact state or local law enforcement to determine whether you can report suspected identify theft relating to this incident. In addition, you can obtain information about avoiding identity theft from the FTC or the Oregon Attorney General's Office. These offices can be reached at:

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

Oregon Department of Justice
Office of the Attorney General
1162 Court St. NE
Salem, OR 97301-4096
(877) 877-9392
https://www.doj.state.or.us/