

MICHELLE A. SCHAAP
mschaap@csglaw.com
(O) 973.530.2026
(F) 973.530.1501

January 31, 2025

Via Email and Certified Mail (Return Receipt Requested)

Maryland Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Re: Notice of Security Incident

To Whom It May Concern:

We serve as legal counsel to One School Global N.A., Inc., with an address at OneSchool Global NA, Inc., 200 Crossing Boulevard, Suite 101, Bridgewater, NJ 08807 (“OSGNA”). This letter¹ serves as notice pursuant to Md. Code Ann., Com. Law § 14-3504(h)(1) regarding a cybersecurity incident (the “Security Incident”) that impacted PowerSchool, a software vendor which provides OSGNA’s Student Information System (“SIS”).²

NATURE OF THE SECURITY INCIDENT

On or about January 9, 2025, PowerSchool first notified OSGNA that it became aware of the Security Incident that occurred on or about December 28, 2024. According to PowerSchool, the Security Incident involved the unauthorized exfiltration of personal information from certain SIS environments through a customer support portal, PowerSource, by an unknown and unauthorized third party.

Notably, the Security Incident impacted many educational institutions’ students and families serviced by PowerSchool. Importantly, the Security Incident is not a result of any fault or vulnerability of OSGNA’s systems or infrastructure, and the data within OSGNA’s own environment and systems were not impacted.

PowerSchool has reported that it has seen no evidence that other PowerSchool products were affected as a result of the Security Incident or that there is any malware or continued unauthorized activity in the PowerSchool environment. Note that OSGNA does not have access to the PowerSchool environment to confirm these statements.

NUMBER AND INFORMATION OF MARYLAND RESIDENTS AFFECTED

At this time, OSGNA believes that the Security Incident resulted in a reportable breach impacting certain individuals, including one (1) Maryland resident enrolled with OSGNA. Specifically, the categories of impacted

¹ Submitted via email and certified mail, as permitted and prescribed at <https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/businessGL.aspx>

² PowerSchool has informed OSGNA that it will be separately and directly notifying impacted individuals.

information include the impacted Maryland resident's first and last name, physical address, doctor's name, doctor's phone number, medications, and previous medical history.

STEPS TAKEN OR PLANNED TO TAKE RELATING TO THE INCIDENT

Since learning of the Security Incident, OSGNA activated its incident response team to determine the scope of the Security Incident. OSGNA continues to communicate with PowerSchool to determine what additional actions PowerSchool is taking to remediate the Security Incident. OSGNA is also informing law enforcement of the Security Incident. To date, OSGNA is not aware of any reports regarding any unauthorized use of personal information beyond the Security Incident. PowerSchool has advised OSGNA that their systems are safe to use and that there is no further risk to their systems.

OSGNA will formally notify the affected Maryland resident of the Security Incident immediately following the delivery of this notice (a copy of the notice is attached hereto). OSGNA will provide the impacted Maryland resident with a copy of the notice via U.S. mail, upon request.

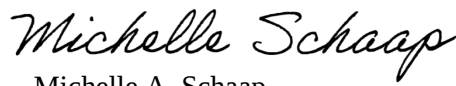
Additionally, PowerSchool has advised OSGNA that, for impacted individuals PowerSchool has sufficient contact information, (i) PowerSchool will provide its own formal notice, additional resources, and complimentary identity protection and credit monitoring services; and (ii) Experian will be distributing a direct email notification on behalf of PowerSchool in the coming weeks with respect to the offer of the two years of complimentary identity protection services. PowerSchool has advised OSGNA that it will also launch a website and distribute a media release to ensure PowerSchool reaches as many impacted individuals as possible and provide them with resources to protect their information. Importantly, these notices will include instructions for impacted individuals on how to enroll in the credit monitoring and identity protection services that are being offered by PowerSchool. Please note that credit monitoring agencies do not offer credit monitoring services for individuals under the age of majority. If a parent or guardian enrolls an impacted individual under the age of majority in the offered identity protection services, the individual, upon reaching the age of majority, will have the opportunity to enroll in credit monitoring services for the duration of the two-year coverage period.

OSGNA will advise the impacted Maryland resident that, to the extent they do not receive such notices from PowerSchool or instructions from Experian, the impacted Maryland resident should contact OSGNA for assistance.

OTHER NOTIFICATION AND CONTACT INFORMATION

Please reach me at 973-530-2026 or mschaap@csglaw.com if you have any questions or need further information.

Respectfully yours,


Michelle A. Schaap

MAS:fxw

Enc. (Sample Personnel Notice issued to the Impacted Individual)

[OSGNA LETTERHEAD]

NOTICE OF DATA BREACH

Dear [**PARENTS**],

At OneSchool Global North America (“OSGNA”), we value transparency and respect the privacy of our students’ and their families’ information.

As a follow up to our January 10, 2025 preliminary notification, we are writing to inform you of the cybersecurity incident (the “**Incident**”) that impacted PowerSchool, a software vendor which provides the Student Information System (“**SIS**”) for OSGNA.

While we are incredibly disappointed by the news of the Incident, we recognize that this news can also be unsettling to impacted students and their families. Please know that we are in contact with PowerSchool to monitor the steps it is taking in response to the Incident.

We are sharing here with you the information we have been provided by PowerSchool as well as pursuant to our own investigation and our understanding of the personal information involved. We are also providing here resources to help protect yourself against possible misuse of the information.

What Happened

On or about January 9, 2025, PowerSchool notified us that it became aware of the Incident that occurred on or about December 28, 2024. According to PowerSchool, the Incident involved the unauthorized exfiltration of personal information from certain SIS environments through a customer support portal, PowerSource, by an unknown and unauthorized third party.

Notably, the Incident impacted not only the information of OSGNA’s students and families but also the information of many educational institutions’ students and families serviced by PowerSchool. Importantly, the Incident is not a result of any fault or vulnerability of OSGNA’s systems or infrastructure, and the data within OSGNA’s own environment and systems were not impacted.

PowerSchool has reported that it has seen no evidence that other PowerSchool products were affected as a result of the Incident or that there is any malware or continued unauthorized activity in the PowerSchool environment. Note that OSGNA does not have access to the PowerSchool environment to confirm these statements.

What Information was Involved

At this time, based on our own investigation and ongoing communications with PowerSchool, we believe that the categories of personally identifiable information impacted by the Incident that results in a reportable breach includes your first and last names and your child’s first and last name, physical address, doctor’s name, doctor’s phone number, medications, and previous medical history.

What We Have Done and What We Are Doing

Since learning of the Incident, we have worked with our incident response team to determine the scope of the Incident. We continue to communicate with PowerSchool to determine what additional actions it is taking to remediate the Incident. We are in the process of informing law enforcement of the Incident. To date, we are not aware of any reports regarding any unauthorized use of personal information beyond the Incident.

PowerSchool has reported that their systems are safe to use and that there is no further risk to their systems. PowerSchool advised that it is providing formal legal notice of the Incident to law enforcement and impacted individuals whose information was determined to be involved.

PowerSchool further advised that it is offering complimentary identity protection and credit monitoring services to all students and their families whose information from OSGNA's PowerSchool SIS was involved. This offer is being provided regardless of whether an individual's Social Security number was exfiltrated.

Identity Protection: PowerSchool will be offering two years of complimentary identity protection services, which will be provided by Experian, for all impacted individuals whose information was involved.

Credit Monitoring: PowerSchool will also be offering two years of complimentary credit monitoring services, which will be provided by TransUnion, for all impacted individuals who have reached the age of majority whose information was involved.

A direct email notification will be distributed by Experian on behalf of PowerSchool in the coming weeks to impacted individuals for whom PowerSchool has sufficient contact information. PowerSchool will also launch a website and distribute a media release to ensure PowerSchool reaches as many impacted individuals as possible and provide them with resources to protect their information.

Importantly, these notices will include instructions for impacted individuals on how to enroll in the credit monitoring and identity protection services that are being offered by PowerSchool.

Please note that credit monitoring agencies do not offer credit monitoring services for individuals under the age of majority. If a parent or guardian enrolls an individual under the age of majority in the offered identity protection services, the individual, upon reaching the age of majority, will have the opportunity to enroll in credit monitoring services for the duration of the two-year coverage period.

If you do not receive such communications from PowerSchool or instructions from both Experian and TransUnion no later than two (2) weeks after receiving this correspondence, please contact us *immediately*.

What You Can Do

Due to the sensitive nature of this information, we want to alert you about potential risks involving your information.

Bad actors may attempt to use this information in phishing scams, potentially referencing specific medical details to appear legitimate. Please be extremely cautious of any unexpected communications that mention this medical information, even if they appear to come from trusted sources.

We strongly recommend you (1) sign up for the complimentary credit monitoring services and complimentary identity protection services offered by PowerSchool, (2) remain vigilant, monitor and review all financial and personal account statements and credit reports, and (3) immediately report any unusual activity to the institution that issued the record and to law enforcement.

Should you receive a call, email, or other communication from someone who claims to have your or your family's personal information:

- Do not engage with the caller/correspondent;
- Listen carefully and immediately following the call, make notes about what you were told; and
- As soon as possible, share the information with support@na.oneschoolglobal.com.

In addition, you can reach out to local law enforcement or your state's attorney general office or consumer protection office. You also have the right to obtain a police report.

For your personal accounts and devices, we strongly recommend that you (i) change your answers to security questions that may use the impacted information, (ii) change default passwords, (iii) use robust passwords and/or passcodes, and do not recycle passwords or use the same password across multiple accounts or devices, and (iv) wherever available on personal devices and accounts, implement two-factor authentication.

Also enclosed with this notice is a resource sheet containing additional information for your general reference, listing toll-free numbers and addresses of the three largest nationwide consumer reporting agencies and Federal Trade Commission.

For More Information

If you have any questions regarding this information, please contact us by telephone (732) 357-7064, by email support@na.oneschoolglobal.com (Subject Line: PowerSchool Incident), or by mail addressed to OneSchool Global NA, Inc., 200 Crossing Boulevard, Suite 101, Bridgewater, NJ 08807.

Kind regards,

Jeff Southard & Jim Admiraal
Regional Managing Directors
One School Global North America

ATTACHMENT

IF YOUR IDENTITY IS COMPROMISED, STEPS YOU CAN TAKE:

- **Local Police Reporting**

File a report with your local police department.

- **Passwords, Passcodes**

Change passwords and passcodes on all personal accounts and devices. Often, people will use the same password that they use for one account or device for multiple accounts and/or devices. If you change passwords, this should include your personal social media accounts, online banking accounts, cellphones, tablets, home computers, etc. Best practice is not to use the same password for more than one account or device, nor to “recycle” or reuse passwords that were used in the last several years. If your accounts offer multi-factor authentication, we suggest you enable this for those accounts.

- **Social Security Administration**

Block Electronic Access: If you know your Social Security information has been compromised, you can request to Block Electronic Access. This is done by calling the Social Security Administration National 800 number (Toll Free 1-800-772-1213 or at our TTY number at 1-800-325-0778). Once requested, any automated telephone and electronic access to your Social Security record is blocked. Note: No one, including you, will be able to see or change your personal information on the internet or through the Social Security Administration’s automated telephone service. If you have requested that the Social Security Administration block access to your record and later change your mind, you can contact the Social Security Administration and ask to have the block removed. You will need to prove your identity when you call the Social Security Administration. See also: <https://www.ssa.gov/pubs/EN-05-10220.pdf>.

- **IRS**

Complete IRS Form 14039. The form can be found at: <https://www.irs.gov/newsroom/tips-for-taxpayers-victims-about-identity-theft-and-tax-returns-2014>. You can contact the IRS Identity Protection Specialized Unit at 1-800-908-4490.

- **Review Your Account Statements and Notify Law Enforcement of Suspicious Activity**

We encourage you to monitor your financial accounts, including the account you use for direct deposit, and ask your account manager for additional services or resources that your bank may offer to protect your accounts. Remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. 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.

We recommend that you review the tips provided by the Federal Trade Commission’s Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at <https://consumer.ftc.gov/identity-theft-and-online-security>. To file with the FTC, go to www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC’s Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies. Theft of your social security number should also be reported to the FTC at <https://www.identitytheft.gov/>.

- **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 a copy of the request form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report, general inquiries, placing a fraud alert on your credit report, or

requesting a credit freeze is provided below:

Experian
1-888-EXPERIAN (397-3742)
P.O. Box 9532
Allen, TX 75013
www.experian.com

TransUnion
1-800-680-7289
Fraud Victim Assistance Division
PO Box 2000
Chester, PA 19016
www.transunion.com

Equifax
1-800-525-6285
P.O. Box 740241
Atlanta, GA 30374-0241
www.equifax.com

- **Fraud Alert**

We recommend placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. 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. 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>.

- **Credit Freezes**

You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit. There is no fee to place or lift a security freeze.

Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security Number
3. Date of birth
4. If you have moved in the past five years, provide the addresses where you have lived during such time
5. Proof of current address such as current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique PIN or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one hour after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specific period of time.

To remove the security freeze, you must submit a request through a toll-free number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze. The credit bureaus have one hour after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

Additional resources may be available from your state. Please see the below listing for your state. Note that not all states have additional sites.

Alabama: The State of Alabama also offers a resource page on identity theft, which can be found at <https://www.revenue.alabama.gov/faqs/if-i-am-a-victim-of-identity-theft-what-should-i-do/>.

Arizona: Arizona's Attorney General Office provides additional information, which can be found at <https://www.azag.gov/consumer/data-breach/identity-theft>.

Arkansas: Arkansas's Attorney General Offices provides additional information, which can be found at <https://arkansasag.gov/consumer-protection/identity/what-should-victims-do/>.

California: The State of California also offers a resource page on identity theft, which can be found at <https://oag.ca.gov/idtheft/facts/victim-checklist>.

Colorado: The State of Colorado also offers a resource page on identity theft, which can be found at: <https://stopfraudcolorado.gov/fraud-center/identity-theft.html>.

Connecticut: The State of Connecticut also offers a resource page on identity theft, which can be found at <https://portal.ct.gov/ag/consumer-issues/identity-theft/identity-theft>.

District of Columbia (DC): The District of Columbia also offers resources on identity theft, which can be found at: <https://oag.dc.gov/consumer-protection/consumer-alert-identity-theft#:~:text=In%20the%20District%20of%20Columbia%2C%20the%20Financial%20and,telephone%20at%20202-727-4159.%20Via%20the%20Internet%20at%20https%3A%2F%2Fwww.mpdcc.gov>

Florida: The State of Florida also offers a resource page on identity theft, which can be found at: <https://www.fdacs.gov/Consumer-Resources/Scams-and-Fraud/Identity-Theft/Identity-Theft>. For additional information, please call the Florida Attorney General's Identity Theft Victim Services toll-free telephone number at 1-866-9-NO-SCAM.

Georgia: The State of Georgia also offers a resource page on identity theft, which can be found at: <https://consumer.georgia.gov/consumer-topics/identity-theft>. See also <https://dds.georgia.gov/georgia-licenseid/existing-licenseid/how-do-i-replace-license>.

Idaho: <https://tax.idaho.gov/guides/protecting-your-identity/identity-theft/>

Illinois: Illinois also offers a resource page on identity theft, which can be found at: <https://www.illinoisattorneygeneral.gov/consumers/hotline.html>

Indiana: The State of Indiana also offers a resource page on identity theft, which can be found at: <https://www.in.gov/attorneygeneral/consumer-protection-division/id-theft-prevention/complaint-form/>

Iowa: <https://www.iowaattorneygeneral.gov/for-crime-victims>

Office of the Attorney General of Iowa
Victim Assistance Section
Hoover State Office Building
1305 East Walnut Street
Des Moines, IA 50319

Phone: 515-281-5044
Toll-Free: 800-373-5044
FAX: 515-281-8199

Kansas: Kansas provides the following resource page: <https://www.ag.ks.gov/divisions/public-protection/your-identity#:~:text=Request%20a%20fraud%20alert&text=Equifax%3A%201%2D800%2D525,1%2D800%2D680%2D7289>

Kentucky: The Commonwealth of Kentucky also offers a resource page on identity theft, which can be found at:

<https://www.ag.ky.gov/Resources/Consumer-Resources/Consumers/Pages/Identity-Theft.aspx>. See also <https://drive.ky.gov/Drivers/Pages/Renew-Replace-Update.aspx>.

Louisiana: The Commonwealth of Louisiana also offers a resource page on identity theft, which can be found at: <https://revenue.louisiana.gov/FraudForms/IdentityTheftChecklist.pdf>

Maryland: Maryland residents may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at <https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx>, or by sending an email to idtheft@oag.state.md.us, or calling 410-576-6491.

Massachusetts: The State of Massachusetts also offers a resource page on identity theft, which can be found at: <https://www.mass.gov/protecting-yourself-if-your-identity-is-stolen>. For additional information, please call the Massachusetts Attorney General's Consumer Advocacy & Response Division, Consumer Hotline at (617) 727-8400.

Michigan: Michigan's Attorney General Office offers additional resources at <https://www.michigan.gov/ag/initiatives/michigan-identity-theft-support>.

Minnesota: The State of Minnesota also offers resource pages on identity theft, which can be found at: <https://dps.mn.gov/divisions/ojp/help-for-crime-victims/Pages/Identity%20Theft.aspx> and also <https://www.revenue.state.mn.us/mndor-pp/6466?type=html>

Mississippi: The State of Mississippi also offers a resource page on identity theft, which can be found at <https://www.its.ms.gov/services/identity-theft>.

Montana: Montana's Department of Justice provides further information at <https://dojmt.gov/consumer/identity-theft/>.

Nebraska: The Nebraska Attorney General provides an Identity Theft Consumer Guide which can be found at [https://protectthegoodlife.nebraska.gov/sites/default/files/doc/Identity Theft June 2023.pdf](https://protectthegoodlife.nebraska.gov/sites/default/files/doc/Identity%20Theft%20June%202023.pdf).

Nevada: Nevada offers resources at https://ag.nv.gov/Hot_Topics/Victims/IDTheft_Victim_Information/.

New Hampshire: New Hampshire's Department of Justice offers a guide for victims of identity theft which can be found at <https://www.doj.nh.gov/citizens/consumer-protection-antitrust-bureau/identity-theft#:~:text=Call%20the%20FTC%27s%20toll%2Dfree,%2D888%2D468%2D4454>.

New Jersey: The State of New Jersey also offers a resource page on identity theft, which can be found at <https://www.nj.gov/njsp/tech/identity.html>.

New Mexico: The New Mexico Department of Justice offers victim resources <https://nm DOJ.gov/about-the-office/criminal-affairs/#victim-services>.

New York: The State of New York also offers a resource page on identity theft, which can be found at: <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>.

North Carolina: North Carolina residents may obtain information about steps you can take to prevent identity theft from the North Carolina Attorney General at <https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/> or by contacting North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001. 877-566-7226 (Toll-free within North Carolina). 919-716-6000.

Ohio: The State of Ohio also offers a resource page on identity theft, which can be found at <https://www.ohioattorneygeneral.gov/identitytheft#>. For the Bureau of Motor Vehicles, see <https://bmvonline.dps.ohio.gov/home/>. For additional information, please visit <https://www.ohioattorneygeneral.gov/FAQ/Responding-to-Identity-Theft-FAQs>.

Oregon: Oregon provides the following resource page with Identity theft protection resources <https://www.oregon.gov/dor/programs/individuals/pages/protecting-your-identity.aspx>.

Oklahoma: The State of Oklahoma also offers a resource page on identity theft, which can be found at: <https://oklahoma.gov/okdhs/library/idresources.html>.

Pennsylvania: The Commonwealth of Pennsylvania also offers a resource page on identity theft, which can be found at: <https://www.attorneygeneral.gov/protect-yourself/identity-theft/>.

Rhode Island: Rhode Island residents may request additional information by contacting: Rhode Island, Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903. Tel: 401-274-4400. Rhode Island also offers a resource page on identity theft, which can be found at <https://riag.ri.gov/what-we-do/civil-division/public-protection/consumer-protection/id-theft>.

South Carolina: The State of South Carolina also offers a resource page on identity theft, which can be found at: <https://consumer.sc.gov/identity-theft-unit/id-theft>.

South Dakota: The State of South Dakota also offers a resource page on identity theft, which can be found at <https://consumer.sd.gov/fastfacts/identitytheft.aspx>.

Tennessee: The State of Tennessee also offers a resource page on identity theft, which can be found at: <https://www.tn.gov/content/dam/tn/safety/documents/IdentityTheftVicrimToolkit.pdf>.

Texas: The State of Texas also offers a resource page on identity theft, which can be found at <https://www.texasattorneygeneral.gov/consumer-protection/identity-theft/identity-theft-resources>.

Utah: Utah offers additional information which can be found at: <https://dcp.utah.gov/education/identity-theft/>. The Utah State Tax Commission also provides resources at: <https://tax.utah.gov/individuals/identity-theft>.

Vermont: The State of Vermont also offers a resource page on identity theft, which can be found at <https://ago.vermont.gov/cap>.

Virginia: The Commonwealth of Virginia also offers a resource page on identity theft, which can be found at: <https://www.oag.state.va.us/programs-outreach/identity-theft>. See also: <https://www.dmv.virginia.gov/licenses-ids/license/applying/identity-theft>.

Washington: Washington State also offers additional information which can be found at: <https://www.atg.wa.gov/recovering-identity-theft-or-fraud>.

West Virginia: The State of West Virginia also offers a resource page on identity theft, which can be found at: <https://ago.wv.gov/consumerprotection/Pages/Identity-Theft-Prevention.aspx>.

Wisconsin: The State of Wisconsin also offers a resource page on identity theft, which can be found at: https://datcp.wi.gov/Pages/Programs_Services/IdentityTheftResources.aspx. See also: <https://datcp.wi.gov/Documents/IDTheftWhatToDo602.pdf>.