Paul T. McGurkin, Jr.
Office: 267-930-4788
Fax: 267-930-4771
Email: pmcgurkin@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

May 17, 2018

VIA EMAIL

Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100
Email: securitybreach@atg.wa.gov

Re: Notice of Data Event

Dear Sir or Madam:

Our office represents Corporation Service Company® ("CSC®"), 251 Little Falls Drive, Wilmington, Delaware 19808-1674. We are writing to provide you with notice of an event that may impact the security of certain personal information relating to approximately 4243 Washington residents. By providing this notice, CSC does not waive any rights or defenses regarding the applicability of Washington law, applicability of the Washington data event notification statute, or personal jurisdiction. CSC's investigation is ongoing and will supplement this notice with any additional material developments.

Nature of the Data Event

CSC provides various services, including domain registration and agent for service of process to its business clients. During the provision of the agent of process services, CSC receives certain personally identifiable information of individuals associated with its various clients directly from the court or party serving the corporation in the legal proceeding. In addition, CSC also receives certain information related to its corporate clients directly from the clients.

During routine security monitoring, CSC detected that an unauthorized third party accessed its network and certain systems. CSC took immediate steps to stop the activity, informed law enforcement, engaged two leading, independent cyber security firms, and notified impacted customers. On April 5, 2018, CSC determined an unknown actor exfiltrated a database table from its network that contained certain personally identifiable information provided by CSC's clients.

While the investigation into this event is ongoing, the data stored with the exfiltrated database table included a combination of the individuals' names and Social Security numbers.

Notice to Washington Residents

On May 17, 2018, CSC will begin providing written notice of this incident to all potentially impacted individuals, which includes 4243 Washington residents. Written notice will be provided in substantially the same form as the letter attached hereto as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon detecting the suspicious activity, CSC quickly initiated incident response and mitigation activities, with the assistance of two leading, independent cyber security investigation firms and law enforcement. In addition, CSC implemented steps, many of which were already in development, to further enhance its security protocols. These included, but were not limited to, requiring two-factor authentication on certain customer facing applications and internal administration logins, expanding web application and other firewalls, and mandating 16-character employee passwords. There is no evidence of current or ongoing unauthorized access to its information or activity in its systems. CSC continues to monitor all systems for unusual activity.

CSC is notifying impacted individuals and offering 12 months of free credit monitoring and identity restoration services. Additionally, CSC is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state attorney general, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of this event, please contact us at 267-930-4788.

Very truly yours,

Paul T. McGurkin of
MULLEN COUGHLIN LLC

PTM/alc
Enclosure

EXHIBIT A

Processing Center ● P.O. BOX 141578 ● Austin, TX 78714

00003
ACD1234

00792
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

May 18, 2018

RE: Notice of Data Breach

Dear John Sample:

Corporation Service Company® ("CSC®"), which provides business, legal, and digital brand services to its customers, is writing to inform you that we recently discovered an incident that may affect the security of certain information relating to you. While we are unaware of any actual or attempted misuse of your information, we are providing this notice to ensure that you are aware of the incident so that you can take steps to protect your information should you feel it is appropriate to do so.

What Happened? During routine security monitoring, we detected that an unauthorized third party accessed parts of our network and certain systems. On April 5, 2018, we determined an unknown actor exfiltrated a database table from our network on November 25, 2017 that contained certain information relating to you.

What Information Was Involved? The information related to you was located within the database and includes your name and Government ID number or Company Business Registration number starting with 303.

What We Are Doing. At CSC, we are constantly working to safeguard our customers' information from rapidly evolving threats. We are also committed to keeping our customers informed. Upon detecting the suspicious activity, we took immediate steps to stop the activity, informed law enforcement, and engaged two leading, independent cyber security investigation firms. In addition, we implemented steps, many of which were already in development, to further enhance our security protocols. These included, but were not limited to, requiring two-factor authentication on certain customer facing applications and internal administration logins, expanding web application and other firewalls, and mandating 16-character employee passwords. There is no evidence of current or ongoing unauthorized access to our information or activity in our systems. We continue to monitor all systems for unusual activity.

We are providing notice of this incident to you, and also offering you complimentary access to 12 months of free credit monitoring and identity restoration services with AllClear ID. We are also notifying certain state regulators and consumer reporting agencies of this incident.

What You Can Do. You can enroll to receive the free credit monitoring and identity restoration services. You can also review the enclosed *Steps You Can Take to Protect Against Identity Theft and Fraud* for information on what you can do to better protect against the possibility of identity theft and fraud.

For More Information. We understand that you may have questions about this letter. To ensure you receive a timely response to any inquiry, we have established a hotline for you to contact us with questions or concerns. This hotline can be reached at 1-855-704-6254 Monday through Saturday 9:00 a.m. to 9:00 p.m. ET.

We regret any inconvenience this incident causes you.

Sincerely,

CSC Privacy Response Unit

Steps You Can Take to Protect Against Identity Theft and Fraud

As an added precaution, we have arranged to have AllClear ID protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-704-6254 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Fraud Alerts with Credit Monitoring: This service offers the ability to set, renew, and remove 90-day fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, a once annual credit score and credit report, and a $1 million identity theft insurance policy. To enroll in this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-704-6254 using the following redemption code: Redemption Code.

Please note: Following enrollment, additional steps are required by you in order to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may also be required in order to activate your monitoring options.

We encourage you to remain vigilant against incidents of identity theft and fraud for the next 12-24 months, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can also have these credit bureaus place a fraud alert on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You can also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for

new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. If you wish to place a freeze on all of your credit files, you will need to do so separately with each of the three major credit bureaus. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
(NY residents call
1-800-349-9960)
www.freeze.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19022-2000
1-888-909-8872
freeze.transunion.com

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state attorney general. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. **For Maryland residents**: the attorney general can be contacted by mail at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; by phone at 1-888-743-0023; and www.oag.state.md.us. **For North Carolina residents**: the attorney general can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov. **For Rhode Island residents**: the attorney general can be contacted by mail at 150 South Main St., Providence, RI 02903; and online at www.riag.ri.gov. Approximately 56 Rhode Island residents may have been affected by this incident. **For New Mexico residents**: you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.