



55 East Monroe Street
37th Floor
Chicago, IL 60603

312 346 7500 main
312 580 2201 fax
thompsoncoburn.com

Melissa K. Ventrone, CIPP/US
312 580 2219 direct
mventrone@thompsoncoburn.com

The Supreme Court of Illinois does not recognize certifications of specialties in the practice of law, and the CIPP/US certificate is not a requirement to practice law in Illinois.

December 2, 2016

Attorney General Joseph Foster
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

Dear Attorney General Foster:

We represent Guilmartin, DiPiro & Sokolowski, LLC ("GDS") with respect to a recent security incident involving the potential exposure of certain personally identifiable information described in more detail below. GDS is an accounting firm based in Middletown, CT, which provides certified public accounting and tax preparation services to its clients.

1. Nature of security incident.

On October 17, 2016, GDS became aware of a possible data incident involving its clients after a GDS tax-preparation software partner alerted GDS that a fraudulent tax return had been filed using GDS' account information. GDS hired a third-party computer forensic firm to analyze GDS' computer servers to determine whether an unauthorized user had gained access to them and the extent of any unauthorized access. On November 2, 2016, the third-party computer forensic firm informed GDS that the server had been accessed by an unauthorized individual, and a specific set of files containing personally identifiable information of a limited number of clients may have been exfiltrated from the GDS computer server.

2. Number of New Hampshire residents affected.

Fourteen (14) New Hampshire residents were affected by the incident. Notification letters were mailed to impacted individuals between December 1, 2016 and December 6, 2016 via regular mail. Enclosed please find a copy of the notification letter.

3. Steps you have taken or plan to take relating to the incident.

GDS has hired a cybersecurity technology company to perform a complete risk assessment of its network and systems, and is working with the technology company to further enhance the security of GDS' systems. GDS has informed the FBI and IRS of its investigation. GDS is also offering potentially impacted individuals 24 months of credit monitoring and identity restoration services through Kroll. Finally, notice was also provided to the credit reporting agencies.

2016 DEC -8 AM 11:37

STATE OF NH
DEPT OF JUSTICE

December 2, 2016
Page 2

4. Contact information.

GDS remains dedicated to protecting the sensitive information in its systems. If you have any questions or need additional information, please do not hesitate to contact me at MVentrone@ThompsonCoburn.com or (312) 580-2219.

Very truly yours,

Thompson Coburn LLP



Melissa K. Ventrone

Enclosures



GUILMARTIN • DIPIRO • SOKOLOWSKI LLC
CERTIFIED PUBLIC ACCOUNTANTS

<<MemberFirstName>> <<MemberLastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

<<Date>> (Format: Month Day, Year)

Notice of Data Breach

Dear <<MemberFirstName>> <<MemberLastName>>,

We are writing to inform you about a data security incident experienced by Guilmartin, DiPiro & Sokolowski, LLC ("GDS") that may have exposed your personal information, including your name and Social Security number. We value and respect the privacy of your information, and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information, and resources we are making available to help you.

1. What happened and what information was involved?

On October 17, 2016 one of GDS' software partners informed GDS that it had detected a fraudulent electronic tax return filing related to one of GDS' clients. GDS immediately began an investigation, and hired a computer forensic company to assist with the investigation. On November 2, 2016, the computer forensic company informed GDS that it appeared that an unauthorized user had gained access to a GDS server and may have accessed files containing your personal information. These files contained information related to your tax return including your name, address, Social Security number, wage information, and possibly your bank account information.

2. What we are doing and what you can do.

To help relieve concerns and restore your confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Identity Consultation, and Identity Restoration.

Visit kroll.idmonitoringservice.com to enroll and take advantage of your Identity monitoring services.

When you visit the link to enroll, use the following Membership Number: <<Member ID>>

Please review the enclosed additional information section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

Additionally, if you know or suspect you are a victim of tax-related identity theft, the IRS recommends the following steps:

- Respond immediately to any IRS notice; call the number provided or, if instructed, go to IDVerify.irs.gov.
- Complete IRS Form 14039, Identity Theft Affidavit. Use a fillable form at IRS.gov, print, then attach the form to your return and mail according to instructions.
- Continue to pay your taxes and file your tax return, even if you must do so by paper.

If you previously contacted the IRS and did not have a resolution, contact the IRS for specialized assistance at 1-800-908-4490. The IRS has teams available to assist. You may also visit <https://www.irs.gov/Individuals/Identity-Protection> for more information.

We want to assure you that we are taking steps to prevent this sort of incident from occurring in the future. We have hired a cybersecurity technology company to perform a complete risk assessment of our network and systems, and are working with the technology company to further enhance the security of our systems. Additionally, we have informed the FBI and IRS of our investigation to help protect you from fraudulent tax filings in the future.

3. For more information.

If you have any questions or concerns, please call 1-???-???-???? Monday through Friday, 9:00 a.m. to 6:00 p.m. Eastern Time (Monday through Friday, excluding major holidays). Your trust is a top priority for Guilmartin, DiPiro & Sokolowski, LLC, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,



Mike DiPiro
Guilmartin, DiPiro & Sokolowski, LLC

U.S. State Notification Requirements

For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina:

It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia:

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report by contacting any one or more of the following national consumer reporting agencies:

Equifax
P.O. Box 105139
Atlanta, GA 30374
1-800-685-1111
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 6790
Fullerton, CA 92834
1-800-916-8800
www.transunion.com

You may also obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon:

State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission.

For residents of Maryland, Illinois, and North Carolina:

You can obtain information from the Maryland and North Carolina Offices of the Attorneys General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

North Carolina Office of the Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.gov

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

For residents of Massachusetts:

It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three credit bureaus is below.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to send a request to each consumer reporting agency by certified mail, overnight mail, or regular stamped mail. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The consumer reporting agency may charge a fee of up to \$5.00 to place a freeze or lift or remove a freeze, but is free if you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency. You may obtain a security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
www.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
<http://www.experian.com/freeze>

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19016
www.transunion.com

More information can also be obtained by contacting the Federal Trade Commission listed above.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ from Kroll:

Credit Monitoring through TransUnion

You'll receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll investigator, who can help you determine if it's an indicator of identity theft.

Identity Consultation

You have unlimited access to consultation with a dedicated licensed investigator at Kroll. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Restoration

If you become a victim of identity theft, an experienced licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and will do most of the work for you. Your investigator can dig deep to uncover all aspects of the identity theft, and then work to resolve it.

¹ Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.