



00001
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

May 12, 2017

NOTICE OF DATA BREACH

Dear John Sample,

We are writing to provide you with information about a data incident involving D'Angelo & Associates, APC.

What Happened?

On Tuesday, April 4, 2017, we encountered suspicious electronic activity in our tax program. We immediately contacted our local IT firm who disabled remote access. An investigation into the matter was commenced and that same day, we notified the IRS and Franchise Tax Board of our findings. We further notified the FBI, and hired a specialized forensic IT firm for additional investigation.

On April 24, 2017, the specialized forensic IT firm determined that there was unauthorized access to our system from a foreign IP address on or before March 25, 2017 through April 15, 2017. Unfortunately, the forensic IT firm cannot determine which files were accessed so we are notifying everyone whose information was accessible out of an abundance of caution.

What Information Was Involved?

If you are an individual, this information may have included your: name, date of birth, telephone number(s), address, Social Security number, all employment (W-2) information, 1099 information (including account number if provided to us), and direct deposit bank account information (including account number and routing information if provided to us).

If you are an entity, this information may have included your: company name, Federal Employer Identification Number, address, telephone number; and partner, shareholder/officer or beneficiary names, addresses, and Social Security numbers.

What We Are Doing.

In addition to notifying the FBI, the IRS, and the FTB, we have notified all three credit bureaus, all applicable state agencies, and we are reviewing office policies and procedures to ensure all security measures are taken to avoid such an incident from occurring again.

As an added precaution, we have also arranged to provide you with 12 months of complimentary identity repair and credit monitoring. Both services start on the date of this notice and you can use them at any time during the next 12 months. However, AllClear Credit Monitoring, which includes a \$1 million identity theft insurance policy, requires you to sign up.



AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-836-1353 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Credit Monitoring: This service has also been prepaid for you for 12 months, but it requires you to enroll. It offers additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. To use this service, you will need to provide your personal information to AllClear ID. Details of the insurance policy can be found at <https://www.allclearid.com/insurance>. To enroll, you may sign up online at enroll.allclearid.com or by phone by calling 1-855-836-1353 using the following redemption code: Redemption Code.

What You Can Do.

In addition to signing-up for the complimentary credit monitoring we have secured for you, given the nature of the information potentially exposed, we recommend that you:

1. Change all bank account numbers that you have provided to us, or at a minimum monitor all such bank activity. These would include direct deposit and electronic fund transfer account details or scanned copies of bank statements and Form 1099's.
2. Establish free 90-day fraud alerts with the three credit reporting bureaus. Their telephone numbers and websites are:

<p>Equifax P.O. Box 740241 Atlanta, GA 30374 1-888-766-0008 https://www.alerts.equifax.com/AutoFraudOnline/jsp/fraudAlert.jsp</p>	<p>Experian P.O. Box 2104 Allen, TX 75013 1-888-397-3742 https://www.experian.com/fraud/center.html</p>	<p>TransUnion P.O. Box 2000 Chester, PA 19022 1-800-680-7289 http://www.transunion.com/fraud-victim-resource/place-fraud-alert</p>
---	--	--

3. Consider placing a credit freeze on your accounts which will make it more difficult for someone to open an account. For more information: <https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs>.
4. If you become a victim or suspect identity theft, file a complaint with the Federal Trade Commission at <https://identitytheft.gov> and law enforcement. The FTC also provides detailed and specific information about identity theft at their website, which we recommend you review.

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

For More Information.

Protecting your information is incredibly important to us, as is addressing this incident with the information and assistance you may need. If you have any questions or concerns, please call toll free number 1-855-836-1353 or write us at 2330 Albatross Street, San Diego, CA 92101.

Very truly yours,

D'Angelo & Associates, APC

Further State Specific Information about Identity Theft Protection

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

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

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

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

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-888-766-0008, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1-800-680-7289, fraud.transunion.com

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit 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 credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC: P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.



AllClear Identity Repair Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- 12 months of coverage with no enrollment required.
- No cost to you — ever. AllClear Identity Repair is paid for by the participating Company.

Services Provided

If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services (“Services”) to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Identity Repair is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period

Service is automatically available to you with no enrollment required for 12 months from the date of the breach incident notification you received from Company (the “Coverage Period”). Fraud Events (each, an “Event”) that were discovered prior to your Coverage Period are not covered by AllClear Identity Repair services.

Eligibility Requirements

To be eligible for Services under AllClear Identity Repair coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim

If you become a victim of fraud covered by the AllClear Identity Repair services, you must:

- Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period;
- Provide proof of eligibility for AllClear Identity Repair by providing the redemption code on the notification letter you received from the sponsor Company;
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require; and
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft.

Coverage under AllClear Identity Repair Does Not Apply to the Following:

Any expense, damage or loss:

- Due to
 - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge, or
 - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your “Misrepresentation”);
- Incurred by you from an Event that did not occur during your coverage period; or
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Identity Repair coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity.
- AllClear ID is not an insurance company, and AllClear Identity Repair is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur.
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud.
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of AllClear Identity Repair coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

Opt-out Policy

If for any reason you wish to have your information removed from the eligibility database for AllClear Identity Repair, please contact AllClear ID:

E-mail support@allclearid.com	Mail AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	Phone 1.855.434.8077
---	--	--------------------------------





01626
TO THE ESTATE OF JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

May 12, 2017

NOTICE OF DATA BREACH

To the Estate of John Sample,

We are writing to provide you with information about a data incident involving D'Angelo & Associates, APC.

What Happened?

On Tuesday, April 4, 2017, we encountered suspicious electronic activity in our tax program. We immediately contacted our local IT firm who disabled remote access. An investigation into the matter was commenced and that same day, we notified the IRS and Franchise Tax Board of our findings. We further notified the FBI, and hired a specialized forensic IT firm for additional investigation.

On April 24, 2017, the specialized forensic IT firm determined that there was unauthorized access to our system from a foreign IP address on or before March 25, 2017 through April 15, 2017. Unfortunately, the forensic IT firm cannot determine which files were accessed so we are notifying everyone whose information was accessible out of an abundance of caution.

What Information Was Involved?

If you are an individual, this information may have included your: name, date of birth, telephone number(s), address, Social Security number, all employment (W-2) information, 1099 information (including account number if provided to us), and direct deposit bank account information (including account number and routing information if provided to us).

If you are an entity, this information may have included your: company name, Federal Employer Identification Number, address, telephone number; and partner, shareholder/officer or beneficiary names, addresses, and Social Security numbers.

What We Are Doing.

In addition to notifying the FBI, the IRS, and the FTB, we have notified all three credit bureaus, all applicable state agencies, and we are reviewing office policies and procedures to ensure all security measures are taken to avoid such an incident from occurring again.

As an added precaution, we have also arranged to provide you with 12 months of complimentary identity repair and credit monitoring. Both services start on the date of this notice and you can use them at any time during the next 12 months. However, AllClear Credit Monitoring, which includes a \$1 million identity theft insurance policy, requires you to sign up.



AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-836-1353 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Credit Monitoring: This service has also been prepaid for you for 12 months, but it requires you to enroll. It offers additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. To use this service, you will need to provide your personal information to AllClear ID. Details of the insurance policy can be found at <https://www.allclearid.com/insurance>. To enroll, you may sign up online at enroll.allclearid.com or by phone by calling 1-855-836-1353 using the following redemption code: Redemption Code.

What You Can Do.

In addition to signing-up for the complimentary credit monitoring we have secured for you, given the nature of the information potentially exposed, we recommend that you:

1. Change all bank account numbers that you have provided to us, or at a minimum monitor all such bank activity. These would include direct deposit and electronic fund transfer account details or scanned copies of bank statements and Form 1099's.
2. Establish free 90-day fraud alerts with the three credit reporting bureaus. Their telephone numbers and websites are:

Equifax P.O. Box 740241 Atlanta, GA 30374 1-888-766-0008 https://www.alerts.equifax.com/AutoFraudOnline/jsp/fraudAlert.jsp	Experian P.O. Box 2104 Allen, TX 75013 1-888-397-3742 https://www.experian.com/fraud/center.html	TransUnion P.O. Box 2000 Chester, PA 19022 1-800-680-7289 http://www.transunion.com/fraud-victim-resource/place-fraud-alert
--	---	---

3. Consider placing a credit freeze on your accounts which will make it more difficult for someone to open an account. For more information: <https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs>.
4. If you become a victim or suspect identity theft, file a complaint with the Federal Trade Commission at <https://identitytheft.gov> and law enforcement. The FTC also provides detailed and specific information about identity theft at their website, which we recommend you review.

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

For More Information.

Protecting your information is incredibly important to us, as is addressing this incident with the information and assistance you may need. If you have any questions or concerns, please call toll free number 1-855-836-1353 or write us at 2330 Albatross Street, San Diego, CA 92101.

Very truly yours,

D'Angelo & Associates, APC

Further State Specific Information about Identity Theft Protection

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

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

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

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

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-888-766-0008, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1-800-680-7289, fraud.transunion.com

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit 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 credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC: P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.



AllClear Identity Repair Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- 12 months of coverage with no enrollment required.
- No cost to you — ever. AllClear Identity Repair is paid for by the participating Company.

Services Provided

If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services (“Services”) to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Identity Repair is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period

Service is automatically available to you with no enrollment required for 12 months from the date of the breach incident notification you received from Company (the “Coverage Period”). Fraud Events (each, an “Event”) that were discovered prior to your Coverage Period are not covered by AllClear Identity Repair services.

Eligibility Requirements

To be eligible for Services under AllClear Identity Repair coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim

If you become a victim of fraud covered by the AllClear Identity Repair services, you must:

- Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period;
- Provide proof of eligibility for AllClear Identity Repair by providing the redemption code on the notification letter you received from the sponsor Company;
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require; and
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft.

Coverage under AllClear Identity Repair Does Not Apply to the Following:

Any expense, damage or loss:

- Due to
 - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge, or
 - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your “Misrepresentation”);
- Incurred by you from an Event that did not occur during your coverage period; or
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Identity Repair coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity.
- AllClear ID is not an insurance company, and AllClear Identity Repair is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur.
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud.
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of AllClear Identity Repair coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

Opt-out Policy

If for any reason you wish to have your information removed from the eligibility database for AllClear Identity Repair, please contact AllClear ID:

E-mail support@allclearid.com	Mail AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	Phone 1.855.434.8077
---	--	--------------------------------





01630
TO THE PARENT OR GUARDIAN OF
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

May 12, 2017

NOTICE OF DATA BREACH

Dear Parent or Guardian of John Sample,

We are writing to provide you with information about a data incident involving D'Angelo & Associates, APC.

What Happened?

On Tuesday, April 4, 2017, we encountered suspicious electronic activity in our tax program. We immediately contacted our local IT firm who disabled remote access. An investigation into the matter was commenced and that same day, we notified the IRS and Franchise Tax Board of our findings. We further notified the FBI, and hired a specialized forensic IT firm for additional investigation.

On April 24, 2017, the specialized forensic IT firm determined that there was unauthorized access to our system from a foreign IP address on or before March 25, 2017 through April 15, 2017. Unfortunately, the forensic IT firm cannot determine which files were accessed so we are notifying everyone whose information was accessible out of an abundance of caution.

What Information Was Involved?

If you are an individual, this information may have included your: name, date of birth, telephone number(s), address, Social Security number, all employment (W-2) information, 1099 information (including account number if provided to us), and direct deposit bank account information (including account number and routing information if provided to us).

If you are an entity, this information may have included your: company name, Federal Employer Identification Number, address, telephone number; and partner, shareholder/officer or beneficiary names, addresses, and Social Security numbers.

What We Are Doing.

In addition to notifying the FBI, the IRS, and the FTB, we have notified all three credit bureaus, all applicable state agencies, and we are reviewing office policies and procedures to ensure all security measures are taken to avoid such an incident from occurring again.

As an added precaution, we have also arranged to provide you with 12 months of complimentary identity repair and credit monitoring. Both services start on the date of this notice and you can use them at any time during the next 12 months. However, AllClear Credit Monitoring, which includes a \$1 million identity theft insurance policy, requires you to sign up.



AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-836-1353 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Credit Monitoring: This service has also been prepaid for you for 12 months, but it requires you to enroll. It offers additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. To use this service, you will need to provide your personal information to AllClear ID. Details of the insurance policy can be found at <https://www.allclearid.com/insurance>. To enroll, you may sign up online at enroll.allclearid.com or by phone by calling 1-855-836-1353 using the following redemption code: Redemption Code.

What You Can Do.

In addition to signing-up for the complimentary credit monitoring we have secured for you, given the nature of the information potentially exposed, we recommend that you:

1. Change all bank account numbers that you have provided to us, or at a minimum monitor all such bank activity. These would include direct deposit and electronic fund transfer account details or scanned copies of bank statements and Form 1099's.
2. Establish free 90-day fraud alerts with the three credit reporting bureaus. Their telephone numbers and websites are:

Equifax P.O. Box 740241 Atlanta, GA 30374 1-888-766-0008 https://www.alerts.equifax.com/AutoFraudOnline/jsp/fraudAlert.jsp	Experian P.O. Box 2104 Allen, TX 75013 1-888-397-3742 https://www.experian.com/fraud/center.html	TransUnion P.O. Box 2000 Chester, PA 19022 1-800-680-7289 http://www.transunion.com/fraud-victim-resource/place-fraud-alert
--	---	---

3. Consider placing a credit freeze on your accounts which will make it more difficult for someone to open an account. For more information: <https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs>.
4. If you become a victim or suspect identity theft, file a complaint with the Federal Trade Commission at <https://identitytheft.gov> and law enforcement. The FTC also provides detailed and specific information about identity theft at their website, which we recommend you review.

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

For More Information.

Protecting your information is incredibly important to us, as is addressing this incident with the information and assistance you may need. If you have any questions or concerns, please call toll free number 1-855-836-1353 or write us at 2330 Albatross Street, San Diego, CA 92101.

Very truly yours,

D'Angelo & Associates, APC

Further State Specific Information about Identity Theft Protection

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

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

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

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

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-888-766-0008, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1-800-680-7289, fraud.transunion.com

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit 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 credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC: P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.



AllClear Identity Repair Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- 12 months of coverage with no enrollment required.
- No cost to you — ever. AllClear Identity Repair is paid for by the participating Company.

Services Provided

If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services (“Services”) to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Identity Repair is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period

Service is automatically available to you with no enrollment required for 12 months from the date of the breach incident notification you received from Company (the “Coverage Period”). Fraud Events (each, an “Event”) that were discovered prior to your Coverage Period are not covered by AllClear Identity Repair services.

Eligibility Requirements

To be eligible for Services under AllClear Identity Repair coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim

If you become a victim of fraud covered by the AllClear Identity Repair services, you must:

- Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period;
- Provide proof of eligibility for AllClear Identity Repair by providing the redemption code on the notification letter you received from the sponsor Company;
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require; and
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft.

Coverage under AllClear Identity Repair Does Not Apply to the Following:

Any expense, damage or loss:

- Due to
 - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge, or
 - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your “Misrepresentation”);
- Incurred by you from an Event that did not occur during your coverage period; or
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Identity Repair coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity.
- AllClear ID is not an insurance company, and AllClear Identity Repair is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur.
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud.
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of AllClear Identity Repair coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

Opt-out Policy

If for any reason you wish to have your information removed from the eligibility database for AllClear Identity Repair, please contact AllClear ID:

E-mail support@allclearid.com	Mail AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	Phone 1.855.434.8077
---	--	--------------------------------





02044
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

May 12, 2017

NOTICE OF DATA BREACH

Dear John Sample,

We are writing to provide you with information about a data incident involving D'Angelo & Associates, APC. You are receiving this letter because you are either a partner, shareholder, or beneficiary of a partnership, company, or trust we performed work for, and accordingly we had some of your personal information in our system.

What Happened?

On Tuesday, April 4, 2017, we encountered suspicious electronic activity in our tax program. We immediately contacted our local IT firm who disabled remote access. An investigation into the matter was commenced and that same day, we notified the IRS and Franchise Tax Board of our findings. We further notified the FBI, and hired a specialized forensic IT firm for additional investigation.

On April 24, 2017, the specialized forensic IT firm determined that there was unauthorized access to our system from a foreign IP address on or before March 25, 2017 through April 15, 2017. Unfortunately, the forensic IT firm cannot determine which files were accessed so we are notifying everyone whose information was accessible out of an abundance of caution.

What Information Was Involved?

As a partner, shareholder, or beneficiary of a partnership, company, or trust we performed work for, the information may have included your: first and last name, address, and Social Security number.

What We Are Doing.

In addition to notifying the FBI, the IRS, and the FTB, we have notified all three credit bureaus, all applicable state agencies, and we are reviewing office policies and procedures to ensure all security measures are taken to avoid such an incident from occurring again.

As an added precaution, we have also arranged to provide you with 12 months of complimentary identity repair and credit monitoring. Both services start on the date of this notice and you can use them at any time during the next 12 months. However, AllClear Credit Monitoring, which includes a \$1 million identity theft insurance policy, requires you to sign up.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-836-1353 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.



AllClear Credit Monitoring: This service has also been prepaid for you for 12 months, but it requires you to enroll. It offers additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. To use this service, you will need to provide your personal information to AllClear ID. Details of the insurance policy can be found at <https://www.allclearid.com/insurance>. To enroll, you may sign up online at enroll.allclearid.com or by phone by calling 1-855-836-1353 using the following redemption code: Redemption Code.

What You Can Do.

In addition to signing-up for the complimentary credit monitoring we have secured for you, given the nature of the information potentially exposed, we recommend that you:

1. Establish free 90-day fraud alerts with the three credit reporting bureaus. Their telephone numbers and websites are:

Equifax P.O. Box 740241 Atlanta, GA 30374 1-888-766-0008 https://www.alerts.equifax.com/AutoFraudOnline/jsp/fraudAlert.jsp	Experian P.O. Box 2104 Allen, TX 75013 1-888-397-3742 https://www.experian.com/fraud/center.html	TransUnion P.O. Box 2000 Chester, PA 19022 1-800-680-7289 http://www.transunion.com/fraud-victim-resource/place-fraud-alert
--	---	---

2. Consider placing a credit freeze on your accounts which will make it more difficult for someone to open an account. For more information: <https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs>.
3. If you become a victim or suspect identity theft, file a complaint with the Federal Trade Commission at <https://identitytheft.gov> and law enforcement. The FTC also provides detailed and specific information about identity theft at their website, which we recommend you review.

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

For More Information.

Protecting your information is incredibly important to us, as is addressing this incident with the information and assistance you may need. If you have any questions or concerns, please call toll free number 1-855-836-1353 or write us at 2330 Albatross Street, San Diego, CA 92101.

Very truly yours,

D'Angelo & Associates, APC

Further State Specific Information about Identity Theft Protection

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

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

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

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

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-888-766-0008, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1-800-680-7289, fraud.transunion.com

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit 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 credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC: P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.



AllClear Identity Repair Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- 12 months of coverage with no enrollment required.
- No cost to you — ever. AllClear Identity Repair is paid for by the participating Company.

Services Provided

If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services (“Services”) to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Identity Repair is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period

Service is automatically available to you with no enrollment required for 12 months from the date of the breach incident notification you received from Company (the “Coverage Period”). Fraud Events (each, an “Event”) that were discovered prior to your Coverage Period are not covered by AllClear Identity Repair services.

Eligibility Requirements

To be eligible for Services under AllClear Identity Repair coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim

If you become a victim of fraud covered by the AllClear Identity Repair services, you must:

- Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period;
- Provide proof of eligibility for AllClear Identity Repair by providing the redemption code on the notification letter you received from the sponsor Company;
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require; and
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft.

Coverage under AllClear Identity Repair Does Not Apply to the Following:

Any expense, damage or loss:

- Due to
 - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge, or
 - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your “Misrepresentation”);
- Incurred by you from an Event that did not occur during your coverage period; or
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Identity Repair coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity.
- AllClear ID is not an insurance company, and AllClear Identity Repair is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur.
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud.
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of AllClear Identity Repair coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

Opt-out Policy

If for any reason you wish to have your information removed from the eligibility database for AllClear Identity Repair, please contact AllClear ID:

E-mail support@allclearid.com	Mail AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	Phone 1.855.434.8077
---	--	--------------------------------





02123
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

May 12, 2017

NOTICE OF DATA BREACH

Dear John Sample,

In follow-up to our prior communications regarding this incident, we are writing to provide you with further information about a data incident involving D'Angelo & Associates, APC.

What Happened?

On Tuesday, April 4, 2017, we encountered suspicious electronic activity in our tax program. We immediately contacted our local IT firm who disabled remote access. An investigation into the matter was commenced and that same day, we notified the IRS and Franchise Tax Board of our findings. We further notified the FBI, and hired a specialized forensic IT firm for additional investigation. Through investigation we determined that your federal tax return was filed by an unauthorized person.

On April 24, 2017, the specialized forensic IT firm determined that there was unauthorized access to our system from a foreign IP address on or before March 25, 2017 through April 15, 2017.

What Information Was Involved?

If you are an individual, this information may have included your: name, date of birth, telephone number(s), address, Social Security number, all employment (W-2) information, 1099 information (including account number if provided to us), and direct deposit bank account information (including account number and routing information if provided to us).

If you are an entity, this information may have included your: company name, Federal Employer Identification Number, address, telephone number; and partner, shareholder/officer or beneficiary names, addresses, and Social Security numbers.

What We Are Doing.

In addition to notifying the FBI, the IRS, and the FTB, we have notified all three credit bureaus, all applicable state agencies, and we are reviewing office policies and procedures to ensure all security measures are taken to avoid such an incident from occurring again.

As an added precaution, we have also arranged to provide you with 12 months of complimentary identity repair and credit monitoring. Both services start on the date of this notice and you can use them at any time during the next 12 months. However, AllClear Credit Monitoring, which includes a \$1 million identity theft insurance policy, requires you to sign up.



AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-836-1353 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Credit Monitoring: This service has also been prepaid for you for 12 months, but it requires you to enroll. It offers additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. To use this service, you will need to provide your personal information to AllClear ID. Details of the insurance policy can be found at <https://www.allclearid.com/insurance>. To enroll, you may sign up online at enroll.allclearid.com or by phone by calling 1-855-836-1353 using the following redemption code: Redemption Code.

What You Can Do.

In addition to signing-up for the complimentary credit monitoring we have secured for you, given the nature of the information potentially exposed, we recommend that you:

1. Change all bank account numbers that you have provided to us, or at a minimum monitor all such bank activity. These would include direct deposit and electronic fund transfer account details or scanned copies of bank statements and Form 1099's.
2. Establish free 90-day fraud alerts with the three credit reporting bureaus. Their telephone numbers and websites are:

<p>Equifax P.O. Box 740241 Atlanta, GA 30374 1-888-766-0008 https://www.alerts.equifax.com/AutoFraudOnline/jsp/fraudAlert.jsp</p>	<p>Experian P.O. Box 2104 Allen, TX 75013 1-888-397-3742 https://www.experian.com/fraud/center.html</p>	<p>TransUnion P.O. Box 2000 Chester, PA 19022 1-800-680-7289 http://www.transunion.com/fraud-victim-resource/place-fraud-alert</p>
---	--	--

3. Consider placing a credit freeze on your accounts which will make it more difficult for someone to open an account. For more information: <https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs>.
4. If you become a victim or suspect identity theft, file a complaint with the Federal Trade Commission at <https://identitytheft.gov> and law enforcement. The FTC also provides detailed and specific information about identity theft at their website, which we recommend you review.

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

For More Information.

Protecting your information is incredibly important to us, as is addressing this incident with the information and assistance you may need. If you have any questions or concerns, please call toll free number 1-855-836-1353 or write us at 2330 Albatross Street, San Diego, CA 92101.

Very truly yours,

D'Angelo & Associates, APC

Further State Specific Information about Identity Theft Protection

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

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

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

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

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-888-766-0008, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1-800-680-7289, fraud.transunion.com

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit 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 credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC: P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.



AllClear Identity Repair Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- 12 months of coverage with no enrollment required.
- No cost to you — ever. AllClear Identity Repair is paid for by the participating Company.

Services Provided

If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services (“Services”) to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Identity Repair is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period

Service is automatically available to you with no enrollment required for 12 months from the date of the breach incident notification you received from Company (the “Coverage Period”). Fraud Events (each, an “Event”) that were discovered prior to your Coverage Period are not covered by AllClear Identity Repair services.

Eligibility Requirements

To be eligible for Services under AllClear Identity Repair coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim

If you become a victim of fraud covered by the AllClear Identity Repair services, you must:

- Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period;
- Provide proof of eligibility for AllClear Identity Repair by providing the redemption code on the notification letter you received from the sponsor Company;
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require; and
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft.

Coverage under AllClear Identity Repair Does Not Apply to the Following:

Any expense, damage or loss:

- Due to
 - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge, or
 - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your “Misrepresentation”);
- Incurred by you from an Event that did not occur during your coverage period; or
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Identity Repair coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity.
- AllClear ID is not an insurance company, and AllClear Identity Repair is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur.
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud.
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of AllClear Identity Repair coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

Opt-out Policy

If for any reason you wish to have your information removed from the eligibility database for AllClear Identity Repair, please contact AllClear ID:

E-mail support@allclearid.com	Mail AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	Phone 1.855.434.8077
---	--	--------------------------------



03-03-5



02173
TO THE PARENT OR GUARDIAN OF
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

May 12, 2017

NOTICE OF DATA BREACH

Dear Parent or Guardian of John Sample,

In follow-up to our prior communications regarding this incident, we are writing to provide you with further information about a data incident involving D'Angelo & Associates, APC.

What Happened?

On Tuesday, April 4, 2017, we encountered suspicious electronic activity in our tax program. We immediately contacted our local IT firm who disabled remote access. An investigation into the matter was commenced and that same day, we notified the IRS and Franchise Tax Board of our findings. We further notified the FBI, and hired a specialized forensic IT firm for additional investigation. Through investigation we determined that your federal tax return was filed by an unauthorized person.

On April 24, 2017, the specialized forensic IT firm determined that there was unauthorized access to our system from a foreign IP address on or before March 25, 2017 through April 15, 2017.

What Information Was Involved?

If you are an individual, this information may have included your: name, date of birth, telephone number(s), address, Social Security number, all employment (W-2) information, 1099 information (including account number if provided to us), and direct deposit bank account information (including account number and routing information if provided to us).

If you are an entity, this information may have included your: company name, Federal Employer Identification Number, address, telephone number; and partner, shareholder/officer or beneficiary names, addresses, and Social Security numbers.

What We Are Doing.

In addition to notifying the FBI, the IRS, and the FTB, we have notified all three credit bureaus, all applicable state agencies, and we are reviewing office policies and procedures to ensure all security measures are taken to avoid such an incident from occurring again.

As an added precaution, we have also arranged to provide you with 12 months of complimentary identity repair and credit monitoring. Both services start on the date of this notice and you can use them at any time during the next 12 months. However, AllClear Credit Monitoring, which includes a \$1 million identity theft insurance policy, requires you to sign up.



AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-836-1353 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Credit Monitoring: This service has also been prepaid for you for 12 months, but it requires you to enroll. It offers additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. To use this service, you will need to provide your personal information to AllClear ID. Details of the insurance policy can be found at <https://www.allclearid.com/insurance>. To enroll, you may sign up online at enroll.allclearid.com or by phone by calling 1-855-836-1353 using the following redemption code: Redemption Code.

What You Can Do.

In addition to signing-up for the complimentary credit monitoring we have secured for you, given the nature of the information potentially exposed, we recommend that you:

1. Change all bank account numbers that you have provided to us, or at a minimum monitor all such bank activity. These would include direct deposit and electronic fund transfer account details or scanned copies of bank statements and Form 1099's.
2. Establish free 90-day fraud alerts with the three credit reporting bureaus. Their telephone numbers and websites are:

Equifax P.O. Box 740241 Atlanta, GA 30374 1-888-766-0008 https://www.alerts.equifax.com/AutoFraudOnline/jsp/fraudAlert.jsp	Experian P.O. Box 2104 Allen, TX 75013 1-888-397-3742 https://www.experian.com/fraud/center.html	TransUnion P.O. Box 2000 Chester, PA 19022 1-800-680-7289 http://www.transunion.com/fraud-victim-resource/place-fraud-alert
--	---	---

3. Consider placing a credit freeze on your accounts which will make it more difficult for someone to open an account. For more information: <https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs>.
4. If you become a victim or suspect identity theft, file a complaint with the Federal Trade Commission at <https://identitytheft.gov> and law enforcement. The FTC also provides detailed and specific information about identity theft at their website, which we recommend you review.

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

For More Information.

Protecting your information is incredibly important to us, as is addressing this incident with the information and assistance you may need. If you have any questions or concerns, please call toll free number 1-855-836-1353 or write us at 2330 Albatross Street, San Diego, CA 92101.

Very truly yours,

D'Angelo & Associates, APC

Further State Specific Information about Identity Theft Protection

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

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

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

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

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-888-766-0008, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1-800-680-7289, fraud.transunion.com

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit 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 credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC: P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.



AllClear Identity Repair Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- 12 months of coverage with no enrollment required.
- No cost to you — ever. AllClear Identity Repair is paid for by the participating Company.

Services Provided

If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services (“Services”) to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Identity Repair is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period

Service is automatically available to you with no enrollment required for 12 months from the date of the breach incident notification you received from Company (the “Coverage Period”). Fraud Events (each, an “Event”) that were discovered prior to your Coverage Period are not covered by AllClear Identity Repair services.

Eligibility Requirements

To be eligible for Services under AllClear Identity Repair coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim

If you become a victim of fraud covered by the AllClear Identity Repair services, you must:

- Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period;
- Provide proof of eligibility for AllClear Identity Repair by providing the redemption code on the notification letter you received from the sponsor Company;
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require; and
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft.

Coverage under AllClear Identity Repair Does Not Apply to the Following:

Any expense, damage or loss:

- Due to
 - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge, or
 - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your “Misrepresentation”);
- Incurred by you from an Event that did not occur during your coverage period; or
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Identity Repair coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity.
- AllClear ID is not an insurance company, and AllClear Identity Repair is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur.
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud.
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of AllClear Identity Repair coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

Opt-out Policy

If for any reason you wish to have your information removed from the eligibility database for AllClear Identity Repair, please contact AllClear ID:

E-mail support@allclearid.com	Mail AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	Phone 1.855.434.8077
---	--	--------------------------------



