



JEFFREY BORN
CPA, INCORPORATED

C/O ID Experts
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

To Enroll, Please Call: 1-800-939-4170 Or Visit: www.IDExpertsCorp.com/protect Enrollment Code: <<XXXXXXXXXX>>
--

<<First name>> <<Last name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

January 26, 2018

Notice of Data Breach

Dear <<First Name>> <<Last Name>>:

Please allow this letter to notify you of a burglary at my office involving two password protected laptops.

What Happened?

On December 31, 2017, I learned that my office was physically broken into and that two password protected laptops were stolen. The Sacramento County Sheriff's Department was immediately called and promptly arrived at the office, investigating the matter. Additionally, I began my own investigation to identify whose and what information was on the devices. The investigation is now complete and I believe that some of your personal information was on one of the stolen password protected laptops. To date, there is still no known access or fraudulent activity, but I want to notify you out of an abundance of caution.

What Information Was Involved?

This may have included your: full name, birthdate, telephone number, address, Social Security number, all employment (W-2) and self-employment information, 1099 information (including account number if provided to my office), entity identification and income earned/amounts received from participation in S-Corp/partnership/LLC/trust, Affordable Care Act insurance data (your medical insurance policy number if you provided us with a Form 1095-A), and direct deposit bank account information (including account number and routing information if provided to my office).

What I Am Doing.

The Sacramento County Sheriff's Department was immediately contacted and I have gone through my records to determine who might be affected. I have also notified the IRS, the FTB, all three credit bureaus and applicable state agencies, and I am reviewing office procedures and security in an attempt to prevent this from occurring again.

As an added precaution, I am offering identity theft protection services through ID Experts®, a data breach and recovery services expert. The MyIDCare™ services include: 12 months of credit monitoring, a \$1,000,000 insurance reimbursement policy, exclusive educational materials, and fully managed identity theft recovery services. With this protection, MyIDCare™ will help you resolve issues if your identity is compromised.

What You Can Do.

I encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling toll free number 1-800-939-4170 or going to <https://www.idexpertscorp.com/protect> and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 6 am - 5 pm Pacific Time. Please note the deadline to enroll is April 26, 2018.

In addition to signing-up for the complimentary credit monitoring I have secured for you, given the nature of the information potentially exposed, you may want to:

1. Change all bank account numbers that you have provided to me, 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 https://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 <https://identitytheft.gov> and law enforcement. The FTC also provides detailed and specific information about identity theft at their website, which I 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 me, as is addressing this incident with the information and assistance you may need. If you have any questions or concerns, please do not hesitate to call toll free number 1-800-939-4170, Monday – Friday, 6 am to 5 pm PST, or call at (916) 973-0677, or write me at 3465 American River Drive, Suite C, Sacramento, CA 95864. Further, you can go to <https://www.idexpertscorp.com/protect> for assistance or for any additional questions you may have.

Sincerely,



Jeffrey Born, CPA

Recommended Steps to Help Protect Your Information

Please Note: Minors, under the age of 18, should not have a credit history established and are under the age to secure credit. Therefore credit monitoring may not be applicable at this time. All other services provided in the membership will apply. No one is allowed to place a fraud alert on your credit report except you, please follow the instructions below to place the alert.

1. Website and Enrollment. Go to <https://www.idexpertscorp.com/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Once you have completed your enrollment, you will receive a welcome letter by email (or by mail if you do not provide an email address when you sign up). The welcome letter will direct you to the exclusive MyIDCare Member Website where you will find other valuable educational information.

2. Activate the credit monitoring provided as part of your MyIDCare membership, which is paid for by Jeffrey Born, CPA. Credit monitoring is included in the membership, but you must personally activate it for it to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

3. Telephone. Contact MyIDCare at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. I recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by visiting their Member website and filing a theft report.

If you file a theft report with MyIDCare, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place 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, P.O. Box 740241, Atlanta, GA 30374

- <https://www.alerts.equifax.com/AutoFraudOnline/jsp/fraudAlert.jsp>

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

- <https://www.experian.com/fraud/center.html>

TransUnion: 1-800-680-7289, P.O. Box 2000, Chester, PA, 19022, fraud.transunion.com

- <https://www.transunion.com/fraud-victim-resource/place-fraud-alert>

If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring.

6. Security Freeze. 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 below.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

- **California Residents:** Visit the California Office of Privacy Protection (www.privacy.ca.gov) for additional information on protection against identity theft.
- **Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TDD: 1-202-326-2502.

To Enroll, Please Call:
1-800-939-4170
Or Visit: www.IDExpertsCorp.com/protect
Enrollment Code: <<XXXXXXXXXX>>

January 26, 2018

[Name]
[Address]
[City, State, Zip]

NOTICE OF DATA BREACH

Dear [NAME]:

Please allow this letter to notify you of a burglary at my office involving two password protected laptops.

What Happened?

On December 31, 2017, I learned that my office was physically broken into and that two password protected laptops were stolen. The Sacramento County Sheriff's Department was immediately called and promptly arrived at the office, investigating the matter. Additionally, I began my own investigation to identify whose and what information was on the devices. The investigation is now complete and I believe that some of your personal information was on one of the stolen password protected laptops. To date, there is still no known access or fraudulent activity, but I want to notify you out of an abundance of caution.

What Information Was Involved?

This may have included trustee and beneficiaries' full names, addresses, Social Security numbers, the trust identification number, grantor Social Security number, 1099 information (including account number if provided to my office), and the beneficiaries' share of income earned and amounts received from the trust.

What I Am Doing.

The Sacramento County Sheriff's Department was immediately contacted and I have gone through my records to determine who might be affected. I have also notified the IRS, the FTB, all three credit bureaus and applicable state agencies, and I am reviewing office procedures and security in an attempt to prevent this from occurring again.

As an added precaution, I am offering identity theft protection services through ID Experts®, a data breach and recovery services expert. The MyIDCare™ services include: 12 months of credit monitoring, a \$1,000,000 insurance reimbursement policy, exclusive educational materials, and fully managed identity theft recovery services. With this protection, MyIDCare™ will help you resolve issues if your identity is compromised.

What You Can Do.

I encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling

toll free number 1-800-939-4170 or going to <https://ide.myidcare.com/protect> and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 6 am - 5 pm Pacific Time. Please note the deadline to enroll is April 26, 2018.

In addition to signing-up for the complimentary credit monitoring I have secured for you, given the nature of the information potentially exposed, you may want to:

1. Change all bank account numbers that you have provided to me, 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 https://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 I 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 me, as is addressing this incident with the information and assistance you may need. If you have any questions or concerns, please do not hesitate to call toll free number 1-800-939-4170, Monday – Friday, 6 am to 5 pm PST, or call at (916) 973-0677, or write me at 3465 American River Drive, Suite C, Sacramento, CA 95864. Further, you can go to <https://ide.myidcare.com/protect> for assistance or for any additional questions you may have.

Sincerely,

Jeffrey Born, CPA

Recommended Steps to Help Protect Your Information

Please Note: Minors, under the age of 18, should not have a credit history established and are under the age to secure credit. Therefore credit monitoring may not be applicable at this time. All other services provided in the membership will apply. No one is allowed to place a fraud alert on your credit report except you, please follow the instructions below to place the alert.

1. Website and Enrollment. Go to <https://ide.myidcare.com/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Once you have completed your enrollment, you will receive a welcome letter by email (or by mail if you do not provide an email address when you sign up). The welcome letter will direct you to the exclusive MyIDCare Member Website where you will find other valuable educational information.

2. Activate the credit monitoring provided as part of your MyIDCare membership, which is paid for by Jeffrey Born, CPA. Credit monitoring is included in the membership, but you must personally activate it for it to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

3. Telephone. Contact MyIDCare at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. I recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by visiting their Member website and filing a theft report.

If you file a theft report with MyIDCare, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

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

If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring.

6. Security Freeze. 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 below.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

- **California Residents:** Visit the California Office of Privacy Protection (www.privacy.ca.gov) for additional information on protection against identity theft.
- **Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TDD: 1-202-326-2502.



JEFFREY BORN
CPA, INCORPORATED

C/O ID Experts
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

<<First name>> <<Last name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

To Enroll, Please Call:
1-800-939-4170
Or Visit: www.IDExpertsCorp.com/protect
Enrollment Code: <<XXXXXXXXXX>>

January 26, 2018

Notice of Data Breach

Dear <<First Name>> <<Last Name>>:

Please allow this letter to notify you of a burglary at my office involving two password protected laptops. You are receiving this letter because you are either a beneficiary, partner, or shareholder of a Jeffrey Born CPA, Inc. client, and therefore some of your information was needed for their tax purposes. Below I have outlined steps I have undertaken, and provided guidance on general best practices for identity theft protection.

What Happened?

On December 31, 2017, I learned that my office was physically broken into and that two password protected laptops were stolen. The Sacramento County Sheriff's Department was immediately called and promptly arrived at the office, investigating the matter. Additionally, I began my own investigation to identify whose and what information was on the devices. The investigation is now complete and I believe that some of your personal information was on one of the stolen password protected laptops. To date, there is still no known access or fraudulent activity, but I want to notify you out of an abundance of caution.

What Information Was Involved?

This may have included your: full name, address, Social Security number, and income earned and amounts received from the client.

What I Am Doing.

The Sacramento County Sheriff's Department was immediately contacted and I have gone through my records to determine who might be affected. I have also notified the IRS, the FTB, all three credit bureaus and applicable state agencies, and I am reviewing office procedures and security in an attempt to prevent this from occurring again.

As an added precaution, I am offering identity theft protection services through ID Experts®, a data breach and recovery services expert. The MyIDCare™ services include: 12 months of credit monitoring, a \$1,000,000 insurance reimbursement policy, exclusive educational materials, and fully managed identity theft recovery services. With this protection, MyIDCare™ will help you resolve issues if your identity is compromised.

What You Can Do.

I encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling toll free number 1-800-939-4170 or going to <https://www.idexpertscorp.com/protect> and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 6 am - 5 pm Pacific Time. Please note the deadline to enroll is April 26, 2018.

In addition to signing-up for the complimentary credit monitoring I have secured for you, given the nature of the information potentially exposed, you may want to:

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 https://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 I 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 me, as is addressing this incident with the information and assistance you may need. If you have any questions or concerns, please do not hesitate to call toll free number 1-800-939-4170, Monday – Friday, 6 am to 5 pm PST, or call at (916) 973-0677, or write me at 3465 American River Drive, Suite C, Sacramento, CA 95864. Further, you can go to <https://www.idexpertscorp.com/protect> for assistance or for any additional questions you may have.

Sincerely,



Jeffrey Born, CPA

Recommended Steps to Help Protect Your Information

Please Note: Minors, under the age of 18, should not have a credit history established and are under the age to secure credit. Therefore credit monitoring may not be applicable at this time. All other services provided in the membership will apply. No one is allowed to place a fraud alert on your credit report except you, please follow the instructions below to place the alert.

1. Website and Enrollment. Go to <https://www.idexpertscorp.com/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Once you have completed your enrollment, you will receive a welcome letter by email (or by mail if you do not provide an email address when you sign up). The welcome letter will direct you to the exclusive MyIDCare Member Website where you will find other valuable educational information.

2. Activate the credit monitoring provided as part of your MyIDCare membership, which is paid for by Jeffrey Born, CPA. Credit monitoring is included in the membership, but you must personally activate it for it to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

3. Telephone. Contact MyIDCare at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. I recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by visiting their Member website and filing a theft report.

If you file a theft report with MyIDCare, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place 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, P.O. Box 740241, Atlanta, GA 30374

- <https://www.alerts.equifax.com/AutoFraudOnline/jsp/fraudAlert.jsp>

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

- <https://www.experian.com/fraud/center.html>

TransUnion: 1-800-680-7289, P.O. Box 2000, Chester, PA, 19022, fraud.transunion.com

- <https://www.transunion.com/fraud-victim-resource/place-fraud-alert>

If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring.

6. Security Freeze. 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 below.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

- **California Residents:** Visit the California Office of Privacy Protection (www.privacy.ca.gov) for additional information on protection against identity theft.
- **Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TDD: 1-202-326-2502.



JEFFREY BORN
CPA, INCORPORATED

C/O ID Experts
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

<<First name>> <<Last name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

To Enroll, Please Call:
1-800-939-4170
Or Visit: www.IDExpertsCorp.com/protect
Enrollment Code: <<XXXXXXXXXX>>

January 26, 2018

Notice of Data Breach

Dear <<First Name>> <<Last Name>>:

Please allow this letter to notify you of a burglary at my office involving two password protected laptops.

What Happened?

On December 31, 2017, I learned that my office was physically broken into and that two password protected laptops were stolen. The Sacramento County Sheriff's Department was immediately called and promptly arrived at the office, investigating the matter. Additionally, I began my own investigation to identify whose and what information was on the devices. The investigation is now complete and I believe that some of your personal information, and that of the trust you represent, was on one of the stolen password protected laptops. To date, there is still no known access or fraudulent activity, but I want to notify you out of an abundance of caution.

What Information Was Involved?

This may have included your: full name, birthdate, telephone number, address, Social Security number, all employment (W-2) and self-employment information, 1099 information (including account number if provided to my office), entity identification and income earned/amounts received from participation in S-Corp/partnership/LLC/trust, Affordable Care Act insurance data (your medical insurance policy number if you provided us with a Form 1095-A), and direct deposit bank account information (including account number and routing information if provided to my office).

Regarding the trust, this may have included trustee and beneficiaries' full names, addresses, Social Security numbers, the trust identification number, grantor Social Security number, 1099 information (including account number if provided to my office), and the beneficiaries' share of income earned and amounts received from the trust.

What I Am Doing.

The Sacramento County Sheriff's Department was immediately contacted and I have gone through my records to determine who might be affected. I have also notified the IRS, the FTB, all three credit bureaus and applicable state agencies, and I am reviewing office procedures and security in an attempt to prevent this from occurring again.

As an added precaution, I am offering identity theft protection services through ID Experts®, a data breach and recovery services expert. The MyIDCare™ services include: 12 months of credit monitoring, a \$1,000,000 insurance reimbursement policy, exclusive educational materials, and fully managed identity theft recovery services. With this protection,

MyIDCare™ will help you resolve issues if your identity is compromised.

What You Can Do.

I encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling toll free number 1-800-939-4170 or going to <https://www.idexpertscorp.com/protect> and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 6 am - 5 pm Pacific Time. Please note the deadline to enroll is April 26, 2018.

In addition to signing-up for the complimentary credit monitoring I have secured for you, given the nature of the information potentially exposed, you may want to:

1. Change all bank account numbers that you have provided to me, 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 https://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 <https://identitytheft.gov> and law enforcement. The FTC also provides detailed and specific information about identity theft at their website, which I 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 me, as is addressing this incident with the information and assistance you may need. If you have any questions or concerns, please do not hesitate to call toll free number 1-800-939-4170, Monday – Friday, 6 am to 5 pm PST, or call at (916) 973-0677, or write me at 3465 American River Drive, Suite C, Sacramento, CA 95864. Further, you can go to <https://www.idexpertscorp.com/protect> for assistance or for any additional questions you may have.

Sincerely,



Jeffrey Born, CPA

Recommended Steps to Help Protect Your Information

Please Note: Minors, under the age of 18, should not have a credit history established and are under the age to secure credit. Therefore credit monitoring may not be applicable at this time. All other services provided in the membership will apply. No one is allowed to place a fraud alert on your credit report except you, please follow the instructions below to place the alert.

1. Website and Enrollment. Go to <https://www.idexpertscorp.com/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Once you have completed your enrollment, you will receive a welcome letter by email (or by mail if you do not provide an email address when you sign up). The welcome letter will direct you to the exclusive MyIDCare Member Website where you will find other valuable educational information.

2. Activate the credit monitoring provided as part of your MyIDCare membership, which is paid for by Jeffrey Born, CPA. Credit monitoring is included in the membership, but you must personally activate it for it to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

3. Telephone. Contact MyIDCare at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. I recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by visiting their Member website and filing a theft report.

If you file a theft report with MyIDCare, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place 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, P.O. Box 740241, Atlanta, GA 30374

- <https://www.alerts.equifax.com/AutoFraudOnline/jsp/fraudAlert.jsp>

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

- <https://www.experian.com/fraud/center.html>

TransUnion: 1-800-680-7289, P.O. Box 2000, Chester, PA, 19022, fraud.transunion.com

- <https://www.transunion.com/fraud-victim-resource/place-fraud-alert>

If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring.

6. Security Freeze. 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 below.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

- **California Residents:** Visit the California Office of Privacy Protection (www.privacy.ca.gov) for additional information on protection against identity theft.
- **Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TDD: 1-202-326-2502.

Letterhead

January 26, 2018

[Name]

[Address]

[City, State, Zip]

NOTICE OF DATA BREACH

Dear [NAME]:

Please allow this letter to notify you of a burglary at my office involving two password protected laptops. You are receiving this letter because you are a trustee of a trust, and you are either a beneficiary, partner, or shareholder of a Jeffrey Born CPA, Inc. client, and therefore some of your information was needed for their tax purposes. Below I have outlined steps I have undertaken, and provided guidance on general best practices for identity theft protection.

What Happened?

On December 31, 2017, I learned that my office was physically broken into and that two password protected laptops were stolen. The Sacramento County Sheriff's Department was immediately called and promptly arrived at the office, investigating the matter. Additionally, I began my own investigation to identify whose and what information was on the devices. The investigation is now complete and I believe that some of your personal information was on one of the stolen password protected laptops. To date, there is still no known access or fraudulent activity, but I want to notify you out of an abundance of caution.

What Information Was Involved?

Regarding the trust, the information may have included the: trustee and beneficiaries' full names, addresses, Social Security numbers, the trust identification number, grantor Social Security number, 1099 information (including account number if provided to my office), and the beneficiaries' share of income earned and amounts received from the trust.

As a beneficiary, partner, or shareholder of a Jeffrey Born CPA, Inc. client, the information may have included your: full name, address, Social Security number, and income earned and amounts received from the client.

What I Am Doing.

The Sacramento County Sheriff's Department was immediately contacted and I have gone through my records to determine who might be affected. I have also notified the IRS, the FTB, all three credit bureaus and applicable state agencies, and I am reviewing office procedures and security in an attempt to prevent this from occurring again.

As an added precaution, I am offering identity theft protection services through ID Experts®, a data breach and recovery services expert. The MyIDCare™ services include: 12 months of credit monitoring, a \$1,000,000 insurance reimbursement policy, exclusive educational materials, and fully

managed identity theft recovery services. With this protection, MyIDCare™ will help you resolve issues if your identity is compromised.

What You Can Do.

I encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling toll free number 1-800-939-4170 or going to <https://ide.myidcare.com/protect> and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 6 am - 5 pm Pacific Time. Please note the deadline to enroll is April 26, 2018.

In addition to signing-up for the complimentary credit monitoring I have secured for you, given the nature of the information potentially exposed, you may want to:

1. Change all bank account numbers that you have provided to me, 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/AutoFraud_Online/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 https://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 I 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 me, as is addressing this incident with the information and assistance you may need. If you have any questions or concerns, please do not hesitate to call toll free number 1-800-939-4170, Monday – Friday, 6 am to 5 pm PST, or call at (916) 973-0677, or write me at 3465 American River Drive, Suite C, Sacramento, CA 95864. Further, you can go to <https://ide.myidcare.com/protect> for assistance or for any additional questions you may have.

Sincerely,

Jeffrey Born, CPA

Recommended Steps to Help Protect Your Information

Please Note: Minors, under the age of 18, should not have a credit history established and are under the age to secure credit. Therefore credit monitoring may not be applicable at this time. All other services provided in the membership will apply. No one is allowed to place a fraud alert on your credit report except you, please follow the instructions below to place the alert.

1. Website and Enrollment. Go to <https://ide.myidcare.com/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Once you have completed your enrollment, you will receive a welcome letter by email (or by mail if you do not provide an email address when you sign up). The welcome letter will direct you to the exclusive MyIDCare Member Website where you will find other valuable educational information.

2. Activate the credit monitoring provided as part of your MyIDCare membership, which is paid for by Jeffrey Born, CPA. Credit monitoring is included in the membership, but you must personally activate it for it to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

3. Telephone. Contact MyIDCare at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. I recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by visiting their Member website and filing a theft report.

If you file a theft report with MyIDCare, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place 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, P.O. Box 740241, Atlanta, GA 30374

- <https://www.alerts.equifax.com/AutoFraudOnline/jsp/fraudAlert.jsp>

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

- <https://www.experian.com/fraud/center.html>

TransUnion: 1-800-680-7289, P.O. Box 2000, Chester, PA, 19022, fraud.transunion.com

- <https://www.transunion.com/fraud-victim-resource/place-fraud-alert>

If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring.

6. Security Freeze. 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 below.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

- **California Residents:** Visit the California Office of Privacy Protection (www.privacy.ca.gov) for additional information on protection against identity theft.
- **Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TDD: 1-202-326-2502.