15701

Sarrell Dental

C/O ID Experts
PO Box 4219
Everett WA 98204

ENDORSE

1 NAME
ADDRESS1
ADDRESS2
CSZ

SEQ
CODE 2D

BREAK

To Enroll, Please Call:
1-833-959-1349
Or Visit:
https://ide.myidcare.com/sarrellprotect
Enrollment Code:
<<XXXXXXXX>>

September 12, 2019

Notice of Data Breach

Dear <<FULL NAME>>,

At Sarrell Dental, we take the security of patient information very seriously, so it is out of an abundance of caution that we are informing you of a data breach that may have resulted in the disclosure of some of your personal health information. We sincerely apologize for any inconvenience this incident may cause. This letter contains information about steps you can take to protect your information and resources we are making available to you.

What Happened
In July 2019, we detected ransomware on Sarrell computers that appears to have been the result of an intrusion that may have begun January 2019. Ransomware is a type of malware usually used by hackers to encrypt a victim's files and demand payment in return for the decryption key. We immediately deactivated our network, temporarily closed our practices, engaged an independent computer security firm to investigate, and did not pay a ransom.

The investigation **has not found evidence that any files or information were copied, downloaded, or removed from our network** as a result of the ransomware. In addition, we have not discovered any evidence that information that may be involved in this incident has been misused. However, because we cannot rule out the possibility that the hackers obtained sensitive information from the network, we are providing you with information about resources to assist you in protecting your information.

What Information Was Involved
The information potentially impacted may include your name, address, date of birth, and health insurance number. **Please note that neither your Social Security Number nor your financial information was involved in this incident.**

What We Are Doing
To protect your health information in the future, we rebuilt our business systems with updated security and virus protection for the entire Sarrell network before reopening our practices. Our network and systems are monitored with upgraded capabilities to ensure that our system and the information we store will remain secure.

We are offering identity theft protection services through ID Experts® to provide you with MyIDCare™. MyIDCare services include 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

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

What You Can Do
We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling 1-833-959-1349 or going to https://ide.myidcare.com/sarrellprotect; and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 8 am - 8 pm Central Time. Please note the deadline to enroll is December 12, 2019.

Again, at this time, we have found no evidence that your information has been misused. Nevertheless, we encourage you to take full advantage of this service offering. MyIDCare representatives can answer any questions or concerns you may have about the protection of your personal information.

You will find detailed instructions for enrollment on the enclosed **Recommended Steps** document. You will need to reference the Enrollment Code at the top of this letter when enrolling online, so be sure to keep this letter.

Sincerely,

Jaqui Melroe
Sarrell Dental Centers

MyIDCare

Recommended Steps to Help Protect Your Information

1. Website and Enrollment. Go to https://ide.myidcare.com/sarrellprotect; and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your MyIDCare membership. The monitoring included in the membership must be activated 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 1-833-959-1349 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. We 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 logging into the MyIDCare website and filing a request for help.

If you file a request for help or report suspicious activity, 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 with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.alerts.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

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 (http://www.ca.gov/Privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

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

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

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), TTY: 1-866-653-4261.

Sarrell Dental

C/O ID Experts
PO Box 4219
Everett WA 98204

ENDORSE

2 NAME
ADDRESS1
ADDRESS2
CSZ BREAK

SEQ
CODE 2D

To Enroll, Please Call:
1-833-959-1349
Or Visit:
https://ide.myidcare.com/sarrellprotect
Enrollment Code:
<<XXXXXXXX>>

September 12, 2019

Notice of Data Breach

Dear <<FULL NAME>>,

At Sarrell Dental, we take the security of patient information very seriously, so it is out of an abundance of caution that we are informing you of a data breach that may have resulted in the disclosure of some of your personal health information. We sincerely apologize for any inconvenience this incident may cause. This letter contains information about steps you can take to protect your information and resources we are making available to you.

What Happened
In July 2019, we detected ransomware on Sarrell computers that appears to have been the result of an intrusion that may have begun January 2019. Ransomware is a type of malware usually used by hackers to encrypt a victim's files and demand payment in return for the decryption key. We immediately deactivated our network, temporarily closed our practices, engaged an independent computer security firm to investigate, and did not pay a ransom.

The investigation **has not found evidence that any files or information were copied, downloaded, or removed from our network** as a result of the ransomware. In addition, we have not discovered any evidence that information that may be involved in this incident has been misused. However, because we cannot rule out the possibility that the hackers obtained sensitive information from the network, we are providing you with information about resources to assist you in protecting your information.

What Information Was Involved
The information potentially impacted may include your name, address, Social Security Number, date of birth, and health insurance number.

What We Are Doing
To protect your health information in the future, we rebuilt our business systems with updated security and virus protection for the entire Sarrell network before reopening our practices. Our network and systems are monitored with upgraded capabilities to ensure that our system and the information we store will remain secure.

We are offering identity theft protection services through ID Experts® to provide you with MyIDCare™. MyIDCare services include 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

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

What You Can Do
We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling 1-833-959-1349 or going to https://ide.myidcare.com/sarrellprotect; and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 8 am - 8 pm Central Time. Please note the deadline to enroll is December 12, 2019.

Again, at this time, we have found no evidence that your information has been misused. Nevertheless, we encourage you to take full advantage of this service offering. MyIDCare representatives can answer any questions or concerns you may have about the protection of your personal information.

You will find detailed instructions for enrollment on the enclosed **Recommended Steps** document. You will need to reference the Enrollment Code at the top of this letter when enrolling online, so be sure to keep this letter.

Sincerely,

Jaqui Melroe
Sarrell Dental Centers

MyIDCare

Recommended Steps to Help Protect Your Information

1. Website and Enrollment. Go to https://ide.myidcare.com/sarrellprotect; and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your MyIDCare membership. The monitoring included in the membership must be activated 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 1-833-959-1349 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. We 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 logging into the MyIDCare website and filing a request for help.

If you file a request for help or report suspicious activity, 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 with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.alerts.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

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 (http://www.ca.gov/Privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

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

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

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), TTY: 1-866-653-4261.

Sarrell Dental

C/O ID Experts
PO Box 4219
Everett WA 98204

ENDORSE

3 NAME
ADDRESS1
ADDRESS2
CSZ

SEQ
CODE 2D

BREAK

To Enroll, Please Call:
1-833-959-1349
Or Visit:
https://ide.myidcare.com/sarrellprotect
Enrollment Code:
<<XXXXXXXX>>

September 12, 2019

Notice of Data Breach

Dear <<FULL NAME>>,

At Sarrell Dental, we take the security of patient information very seriously, so it is out of an abundance of caution that we are informing you of a data breach that may have resulted in the disclosure of some of your personal health information. We sincerely apologize for any inconvenience this incident may cause. This letter contains information about steps you can take to protect your information and resources we are making available to you.

What Happened
In July 2019, we detected ransomware on Sarrell computers that appears to have been the result of an intrusion that may have begun January 2019. Ransomware is a type of malware usually used by hackers to encrypt a victim's files and demand payment in return for the decryption key. We immediately deactivated our network, temporarily closed our practices, engaged an independent computer security firm to investigate, and did not pay a ransom.

The investigation **has not found evidence that any files or information were copied, downloaded, or removed from our network** as a result of the ransomware. In addition, we have not discovered any evidence that information that may be involved in this incident has been misused. However, because we cannot rule out the possibility that the hackers obtained sensitive information from the network, we are providing you with information about resources to assist you in protecting your information.

What Information Was Involved
The information potentially impacted may include your name, address, date of birth, health insurance number, and treatment information including dates of service, diagnosis codes, procedure codes and treating provider. **Please note that neither your Social Security Number nor your financial information was involved in this incident.**

What We Are Doing
To protect your health information in the future, we rebuilt our business systems with updated security and virus protection for the entire Sarrell network before reopening our practices. Our network and systems are monitored with upgraded capabilities to ensure that our system and the information we store will remain secure.

We are offering identity theft protection services through ID Experts® to provide you with MyIDCare™. MyIDCare services include 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

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

What You Can Do
We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling 1-833-959-1349 or going to https://ide.myidcare.com/sarrellprotect; and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 8 am - 8 pm Central Time. Please note the deadline to enroll is December 12, 2019.

Again, at this time, we have found no evidence that your information has been misused. Nevertheless, we encourage you to take full advantage of this service offering. MyIDCare representatives can answer any questions or concerns you may have about the protection of your personal information.

You will find detailed instructions for enrollment on the enclosed **Recommended Steps** document. You will need to reference the Enrollment Code at the top of this letter when enrolling online, so be sure to keep this letter.

Sincerely,

Jaqui Melroe
Sarrell Dental Centers

MyIDCare

Recommended Steps to Help Protect Your Information

1. Website and Enrollment. Go to https://ide.myidcare.com/sarrellprotect; and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your MyIDCare membership. The monitoring included in the membership must be activated 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 1-833-959-1349 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. We 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 logging into the MyIDCare website and filing a request for help.

If you file a request for help or report suspicious activity, 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 with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.alerts.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need

to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

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 (http://www.ca.gov/Privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

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

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center
Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

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), TTY: 1-866-653-4261.

Sarrell Dental

C/O ID Experts
PO Box 4219
Everett WA 98204

ENDORSE

4 NAME
ADDRESS1
ADDRESS2
CSZ

SEQ
CODE 2D

BREAK

To Enroll, Please Call:
1-833-959-1349
Or Visit:
https://ide.myidcare.com/sarrellprotect
Enrollment Code:
<<XXXXXXXX>>

September 12, 2019

Notice of Data Breach

Dear <<FULL NAME>>,

At Sarrell Dental, we take the security of patient information very seriously, so it is out of an abundance of caution that we are informing you of a data breach that may have resulted in the disclosure of some of your personal health information. We sincerely apologize for any inconvenience this incident may cause. This letter contains information about steps you can take to protect your information and resources we are making available to you.

What Happened
In July 2019, we detected ransomware on Sarrell computers that appears to have been the result of an intrusion that may have begun January 2019. Ransomware is a type of malware usually used by hackers to encrypt a victim's files and demand payment in return for the decryption key. We immediately deactivated our network, temporarily closed our practices, engaged an independent computer security firm to investigate, and did not pay a ransom.

The investigation **has not found evidence that any files or information were copied, downloaded, or removed from our network** as a result of the ransomware. In addition, we have not discovered any evidence that information that may be involved in this incident has been misused. However, because we cannot rule out the possibility that the hackers obtained sensitive information from the network, we are providing you with information about resources to assist you in protecting your information.

What Information Was Involved
The information potentially impacted may include your name, address, Social Security Number, date of birth, health insurance number, and treatment information including dates of service, diagnosis codes, procedure codes and treating provider.

What We Are Doing
To protect your health information in the future, we rebuilt our business systems with updated security and virus protection for the entire Sarrell network before reopening our practices. Our network and systems are monitored with upgraded capabilities to ensure that our system and the information we store will remain secure.

We are offering identity theft protection services through ID Experts® to provide you with MyIDCare™. MyIDCare services include 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

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

What You Can Do
We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling 1-833-959-1349 or going to https://ide.myidcare.com/sarrellprotect; and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 8 am - 8 pm Central Time. Please note the deadline to enroll is December 12, 2019.

Again, at this time, we have found no evidence that your information has been misused. Nevertheless, we encourage you to take full advantage of this service offering. MyIDCare representatives can answer any questions or concerns you may have about the protection of your personal information.

You will find detailed instructions for enrollment on the enclosed **Recommended Steps** document. You will need to reference the Enrollment Code at the top of this letter when enrolling online, so be sure to keep this letter.

Sincerely,

Jaqui Melroe
Sarrell Dental Centers

MyIDCare

Recommended Steps to Help Protect Your Information

1. Website and Enrollment. Go to https://ide.myidcare.com/sarrellprotect; and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your MyIDCare membership. The monitoring included in the membership must be activated 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 1-833-959-1349 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. We 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 logging into the MyIDCare website and filing a request for help.

If you file a request for help or report suspicious activity, 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 with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.alerts.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need

to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

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 (http://www.ca.gov/Privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

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

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

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), TTY: 1-866-653-4261.