BSF | BOIES SCHILLER FLEXNER

MICHAEL GOTTLIEB
Tel.: (202) 237-2727
E-mail: mgottlieb@bsfllp.com

October 25, 2018

Consumer Protection and Antitrust Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
Phone: (603) 271-3643
Fax: (603) 271-2110

SENT VIA FAX

RE: Data Breach Notification

To Whom It May Concern:

Pursuant to N.H. Rev. Stat. § 359-C:19 et seq. (the "Act"), Net32, Inc. hereby provides notice to the of a security breach under the Act.

Who Is Net32?

Net32 is an online marketplace for the sale of dental supplies and equipment, connecting dentists and dental practices around the country with manufacturers and distributors of dental supplies and equipment. When customers place orders with Net32, Net32 collects their payment and order information and stores it in an order management system. The vendor or supplier that will fulfill the order then logs into the order management system, views the orders placed with them, processes the payment for the order, and ships the goods.

Background Of The Incident

Based on its ongoing forensic investigation, Net32 has discovered that one of Net32's third-party vendors had its log-in credentials to the Net32 platform misused to access Net32's order management system improperly between September 22, 2018, and September 25, 2018. These credentials appear to have been used to generate anomalous order activity for old orders placed with that vendor in a way that revealed credit card information to the user of the vendor's credentials. During this four-day period, customers began reporting to Net32 increased incidents of what appeared to be fraudulent charges relating to the credit cards used to make purchases from this vendor. After learning of the anomalous order activity and the

BSF

increased fraud reports, Net32 suspended the vendor's credentials on September 25, 2018. Net32 also required all vendors to reset their passwords at this time.

What Information Was Involved

Net32 believes that certain personal information relating to Net32 orders may have been exposed, potentially including credit card numbers used to place one vendor's orders on the Net32 platform. We have no reason to believe that any personal information that is not associated with Net32 orders, such as social security numbers, was affected by the breach.

Impact Of The Incident In New Hampshire

While Net32 is working to confirm the precise number of individuals impacted by this security breach, Net32 believes there are no more than 51 New Hampshire customers impacted by the breach. Net32 sent a preliminary email notification to these customers on September 29, 2018.

Steps Taken After The Incident

Net32 takes its customers' privacy and the security of its systems very seriously. Net32 has engaged outside counsel and a cybersecurity forensic firm, and is working with the affected vendor to investigate this incident and ensure that similar incidents cannot occur in the future. Net32 has required all vendors to change their credentials, and has implemented new requirements for how vendors must treat their credentials on a going-forward basis. Net32 is also in the process of changing how customer orders are stored and processed so that additional protections of customers' personal information will be in place even if, in the future, a vendor's credentials are compromised.

A copy of the notice Net32 has provided to New Hampshire consumers via mail on October 25, 2018 is attached. Please let me or my colleague Jon Knight (tel. 202-895-7567, jknight@bsfllp.com) know if you have any further questions regarding this matter.

Sincerely,

/s/ Michael Gottlieb

Michael Gottlieb
Counsel for Net32, Inc.

Net32
250 Towne Village Dr.
Cary, NC 27513

October 25, 2018

##E1419-L01-0123456
SAMPLE A SAMPLE
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

RE: Important Security Notification
Please read this entire letter.

Dear Sample A Sample:

On September 29, 2018, we contacted you via email regarding a data security incident that occurred on or around September 22, 2018 at Net32. The purpose of this letter is to update you on the additional steps we have taken to address the incident and to protect you and your information.

What happened:

Based on its ongoing forensic investigation, Net32 has discovered that one of Net32's third-party vendors had its log-in credentials to the Net32 platform misused to improperly access Net32's order management system between September 22, 2018, and September 25, 2018. These credentials appear to have been used to generate anomalous order activity for old orders placed with that vendor in a way that revealed credit card information to the user of the vendor's credentials. During this four-day period, customers began reporting to Net32 increased incidents of what appeared to be fraudulent charges relating to the credit cards used to make purchases from this vendor. After learning of the anomalous order activity and the increased fraud reports, Net32 suspended the vendor's credentials on September 25, 2018. Net32 also required all vendors to reset their passwords at this time.

What Information Was Involved:

As we stated in our September 29 notice, we believe that certain personal information relating to Net32 orders may have been exposed, potentially including credit card numbers used to place one vendor's orders on the Net32 platform. We do not believe any personal information that is not associated with Net32 orders, such as social security numbers, would have been affected by the breach.

0123456

What We Are Doing:

We have required all vendors to change their credentials and we have implemented new requirements for how vendors must treat their credentials. We are also in the process of changing how customer orders are stored and processed so that even if a vendor's credentials are compromised, this type of improper access to customer

E1419-L01

personal information should not occur. Additionally, we have partnered with Experian to provide free credit monitoring service to all customers who have found potentially fraudulent charges on their accounts. In the event you have had such charges, please contact Net32 by emailing support@net32.com or calling 1-800-517-1997

What You Can Do:

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

More Information:

We sincerely apologize for this incident and regret any inconvenience it may cause you. Should you have questions or concerns regarding this matter, please do not hesitate to contact us at support@net32.com or 1-800-517-1997 between 6 AM EST and 8 PM EST.

Sincerely,

Pat Cassidy

Pat Cassidy, DMD, MPH
CEO, Net32 Inc.
250 Towne Village Drive
Cary, NC 27513

Reference Guide

We encourage you to take the following steps:

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information cannot be explained, then you will need to call the creditors involved. Information that cannot be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Report Incidents. If you detect any unauthorized transactions in a payment card account, promptly notify your relevant payment card issuer or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement or your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. For streamlined checklists and sample letters to help guide you through the recovery process, please visit https://www.identitytheft.gov/.

- File a police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

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

0123456

E1419-L01

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax Equifax Credit Information Services, Inc. 1-800-525-6285 www.equifax.com P.O. Box 740241 Atlanta, GA 30374	Experian Experian Inc. 1-888-397-3742 www.experian.com P.O. Box 9554 Allen, TX 75013	TransUnion TransUnion LLC 1-800-680-7289 www.transunion.com P.O. Box 2000 Chester, PA 19022-2000

Consider Placing a Security Freeze on Your Credit File. You may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually. For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

Additional Information:

For residents of Massachusetts and Rhode Island. It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of Connecticut, Massachusetts, Rhode Island, and West Virginia. You also have the right to place a security freeze on your credit report by contacting any of the credit bureaus listed at above. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a

security freeze on your credit report, you may be able to use an online process, an automated telephone line or a written request. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The consumer reporting agency may charge a fee of up to $5.00 to place a freeze or lift or remove a freeze and free if you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency.

For residents of Iowa, Maryland, Michigan, Missouri, North Carolina, Oregon, and West Virginia. It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account.

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

For residents of Oregon. State laws advise you to report any suspected identity theft to law enforcement, as well as the Attorney General and Federal Trade Commission.

For residents of Illinois, Maryland, Rhode Island and North Carolina. You can obtain information from your respective state Offices of the Attorney General, about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

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

Rhode Island Office of the Attorney General Consumer Protection Unit (401) 274-4400
http://www.riag.ri.gov

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