

July 21, 2017

Gregory J. Bautista
914.872.7839 (direct)
Gregory.Bautista@wilsonelser.com

Attorney General Xavier Becerra
Office of the Attorney General
California Department of Justice
Attn: Public Inquiry Unit
P.O. Box 944255
Sacramento, CA 94244-2550

Re: Data Security Incident

Dear Attorney General Becerra:

We represent Value Eyecare Network, Inc. d/b/a 39dollarglasses.com (“39DollarGlasses”), located in Hauppauge, New York, with respect to a potential data security incident described in more detail below. 39DollarGlasses takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar incident from occurring in the future.

1. Nature of security incident.

On June 8, 2017, 39DollarGlasses learned that an unknown individual may have captured customer payment card information used to make purchases at its online store. 39DollarGlasses immediately took action and commenced an investigation to determine what information may have been accessed. 39DollarGlasses determined that the unknown individual may have accessed some of its customer names, addresses, telephone numbers, and credit/debit card information.

2. Number of California residents affected.

Approximately fourteen thousand, six hundred and forty-seven (14,647) California residents may have been potentially affected by this incident. Notification letters to these individuals were mailed on July 21, 2017, by first class mail. A sample copy of the notification letter is included with this letter.

3. Steps taken relating to the potential incident.

39DollarGlasses has taken steps to prevent a similar event from occurring in the future, and to protect the privacy and security of customer information. These actions include re-coding and relocating its website to a more secure web environment, and implementing additional security measures that ensure customer transactions remain secure. 39DollarGlasses is also offering potentially impacted customers identity theft

1133 Westchester Avenue • White Plains, NY 10604 • p 914.323.7000 • f 914.323.7001

Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston • Indiana • Kentucky
Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • New Jersey • New Orleans • New York • Orlando • Philadelphia • San Diego • San Francisco
Stamford • Virginia • Washington, DC • West Palm Beach • White Plains

wilsonelser.com

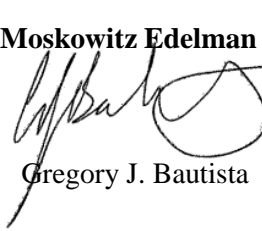
protection services for one year, at no cost to the individual, through AllClear ID. Notice is also being provided to the credit reporting agencies.

4. Contact information.

39DollarGlasses remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please contact me at Gregory.Bautista@wilsonelser.com or (914) 872-7839.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Gregory J. Bautista

Enclosure



100239
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

July 21, 2017

Re: Notice of Data Breach

Dear John Sample:

We would like to thank you for being a loyal customer of 39dollarglasses.com. The company was started over 16 years ago with the goal of ensuring quality prescription eyewear is affordable to everyone. In keeping with this goal of looking out for our customers, we are writing to inform you of an incident that may have resulted in the disclosure of your name and payment card information. We have already resolved this issue. The website has been re-coded (i.e. rebuilt) and moved to a completely new web environment with the highest security standards. The incident occurred prior to making this move. It is described below, as well as steps you can take to protect yourself.

What happened and what information was involved:

On June 8, 2017, we learned that an unknown individual may have accessed your credit or debit card information used to make purchases at our online store. We immediately took action and commenced an investigation to determine what information may have been accessed. We determined that the unknown individual may have accessed customer payment card information, including name, address, telephone number, and credit/debit card information. The potentially compromised information did not include your Social Security number, date of birth or prescription information.

What we are doing and what you can do:

Although our investigation indicated that only a very small percentage of cards may have been impacted, we recommend that you check your current and past credit or debit card statements for unusual or suspicious activity, and if any is found, report it to your bank or credit card company. Additional tips for protecting your information can be found within the enclosed insert.

As an added precaution, we have arranged to have AllClear ID protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-865-4456, provide your Reference Code Redemption Code, and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

We want to assure you that we have taken steps to prevent a similar event from occurring in the future, and to protect the privacy and security of your information. We have relocated our website to a more secure web environment and implemented additional security measures that ensure your transactions remain secure.



For more information:

Please know that the protection and security of your personal information is our utmost priority, and we sincerely regret any inconvenience or concern this matter may cause you. As a thank you for being a loyal customer, we would like to offer you 30% off on all orders through August 15th, 2017 using code **thankyou30**. If you have any questions or concerns, please call 1-855-865-4456, Monday through Saturday, 9:00 a.m. to 9:00 p.m. (Eastern).

Sincerely,

39DollarGlasses.com

Additional Important Information

For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

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

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the nationwide three credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa:

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

For residents of Oregon:

State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, and North Carolina:

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

Maryland Office of the Attorney General

Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

Rhode Island Office of the Attorney General

Consumer Protection
150 South Main Street
Providence RI 02903
1-401-274-4400
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

Federal Trade Commission

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

For residents of Massachusetts:

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

For residents of all states:

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

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

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, or regular stamped mail, or by following the instructions found at the websites listed below. 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 small fee to place, life, or remove a freeze, but is free if you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency. You may obtain a security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348
www.freeze.equifax.com
1-800-525-6285

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
1-888-397-3742

TransUnion (FVAD)

P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
1-888-680-7289

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



AllClear Identity Repair Terms of Use

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

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

Services Provided

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

Coverage Period

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

Eligibility Requirements

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

How to File a Claim

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

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

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

Any expense, damage or loss:

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

Other Exclusions:

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

Opt-out Policy

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

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

