From: Pearl Keng <pearlkeng@gmail.com>
Sent: Monday, September 16, 2019 9:00 PM
To: DOJ: Attorney General <attorneygeneral@doj.nh.gov>
Subject: New Hampshire Notice of Security Breach (Attn: Attorney General Gordon MacDonald)

_____

Dear Attorney General MacDonald:

Dear Attorney General MacDonald:

Pursuant to NH Rev Stat Section 359-C:20, I am providing you notice with a recent breach of my client's website. Attached is a copy of the notice letter which will be mailed out by the end of this week (Sept. 20). There are approximately 16 customers affected in New Hampshire.

The information compromised was customer name, credit card numbers, and passwords for those cards. This information was illegally accessed during the transmission to the third party vendor, PNC, who is the merchant servicer managing the transactions . The breach occurred on Accurate Word's website, not the merchant servicer's site. We have notified PNC of this breach.

Accurate Word received a call from Georgetown University whose IT people traced an unauthorized charge on a card to the Accurate Word website. We have since taken steps to remedy this and prevent it from happening again.

Specifically, our investigation showed the attacker used RDP to gain access through the BlueKeep exploit. Microsoft had issued a patch for the BlueKeep exploit back in May 2019 and we had applied the BlueKeep patch but the hacker breached the patched system through RDP using malformed SSL packets.

We have since blocked access to port 3389 (RDP) except for a couple of explicit IP addresses using a firewall in front of the RDP port. We have checked ASP web files to ensure that the hacker has not changed them. We found 1 file altered by the hacker, but it is now secure. We found Excel dump payload and removed it and updated 604 files with routine to force all pages to deliver only with HTTPS (SSL). Finally, we have checked the server daily since closing breach on August 16, 2019 and no additional breaches have been seen. A total of only two incidents of unauthorized charges have been reported.

If you need any additional information, please let me know.

Thank you,

Pearl Keng
Pearl Keng, Esq.
1200 G Street, N.W.
Suite 800
Washington, D.C. 20005
Telephone: (301) 672-2894
Email: pearlkeng@gmail.com

***

NEW HAMPSHIRE – NOTICE OF SECURITY BREACH

Dear Valued Customer:

According to our records, you ordered business cards online. Please be advised that you are receiving this notice pursuant to New Hampshire, Right to Privacy Chapter 359-C, Notice of Security Breach Required, NH Rev Stat § 359-C:20 (2015).

WHAT HAPPENED: On August 16, 2019, our company was notified of a breach, which occurred on or about the same day, of the security of its system. The company conducted an investigation on August 16, 2019 to determine the likelihood that personal information of its individual customers had been or would be misused as a result of the breach. After the investigation concluded, only two instances of actual misuse were found, but out of an abundance of precaution against the possibility that the breach of its security system created a likelihood that your personal information has been or will be misused, we are notifying all our customers of the breach.

WHAT INFORMATION WAS INVOLVED: Names, account numbers, and passwords to your credit card which you used to purchase products or services (business cards) from our company may have been accessed by the breach we experienced.

WHAT WE ARE DOING: Our company has blocked access to our system and checked ASP web files to ensure that the hacker has not changed them. Finally, we have checked the server daily since closing break on August 16, 2019 and no additional breaches have been seen.

FOR MORE INFORMATION CONTACT INFORMATION

Accurate Word, LLC
Address: 4481 White Plains Ln, White Plains, MD 20695
Phone - (301) 539-4970
Email – IDreport@accurateword.com

WHAT YOU CAN DO: It is recommended you change your password for the credit card account that was breached, or have the card canceled and reissued. Also contact the major consumer reporting agencies to advise them of this situation and – as a part of your remediation efforts – use their services to monitor your credit and/or inquire about a fraud alert, please note the following contact information for those reporting agencies:

Equifax
Online - https://my.equifax.com/consumer-registration
Phone: 1-888-836-6351, 1-800-685-1111 / **Automated Service Line** 800-525-6285
Mail
Equifax Information Services LLC
P.O. Box 105069
Atlanta, GA 30348-5069

TransUnion
Online: https://www.transunion.com/fraud-alerts
Phone: 1-800-680-7289, 1-888-909-8872
Mail:
TransUnion Fraud Victim Assistance
P.O. Box 2000
Chester, PA 19016

Experian
Online - https://www.experian.com/ncaconline/fraudalert
Phone – 1-888-397-3742
Mail:
Experian

P.O. Box 4500
Allen, TX 75013

Furthermore, you can obtain information about identity theft from the following agencies:

Federal Trade Commission
Headquarters - 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580
Telephone: (202) 326-2222
Online - https://identitytheft.gov/

- File a complaint with the FTC by calling the ID Theft Hotline: 1-877-IDTHEFT (1-877-438-4338)
- Visit - http://www.consumer.ftc.gov/features/feature-0016-protect-your-identity-event-kit

New Hampshire Office of the Attorney General
Online - https://www.doj.nh.gov/
New Hampshire Department of Justice
33 Capitol Street | Concord, NH | 03301
Telephone: 603-271-3658 / Email - Email: attorneygeneral@doj.nh.gov
Consumer Protection Hotline
1-888-468-4454 or (603) 271-3641
Weekdays 9am to 3pm
DOJ-CPB@doj.nh.gov
Contact information for the Consumer Protection Bureau
Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
Phone: (603) 271-3643
Fax: (603) 271-2110
Additional Resources: https://www.doj.nh.gov/consumer/identity-theft/resources.htm
Credit Report: https://www.annualcreditreport.com/index.action

Police Reports
Contact your local police department to file a report. The report may be filed in the location in which the offense occurred, or the city or county in which you reside. When you file the report, provide as much documentation as possible, including copies of debt collection letters, credit reports, and your notarized ID Theft Affidavit.
Also you can visit the FBI Internet crime complaint Website - https://www.ic3.gov/default.aspx.

HOW TO PROTECT YOURSELF

Because protecting your personal information is important, we take this opportunity to provide you with some additional information and resources which offer guidance on how to protect yourself in the future. According to the Federal Trade Commission (FTC), the following are factors to consider when it comes to identity theft protection:

- Keep your personal information secure offline. Consider limiting the personal documents you carry, and cross-shred documents that may contain personal or sensitive information, such as receipts, charge cards, and financial statements;
- Keep your personal information secure online. Among the behaviors you may want to consider when it comes to your personal information online, the FTC recommends that consumers avoid sharing passwords – even with friends and family – and suggests being extremely careful about the information you share on social networks.
- Secure your Social Security number. Avoid carrying around your Social Security card, and if someone asks you to share your number or your child's number, ask how it will be used, how it will be safeguarded, and why it is needed.

- Keep your devices secure. Before sharing your personal information over public WiFi, understand how your information will be protected. Always lock up your devices, and stay current on the anti-virus software you may have installed on your devices.

You cannot simply change your name, Social Security number, or date of birth. Therefore, we encourage you to take several steps to protect yourself and your loved ones. Below are suggestions regarding what you can do:

1. **Monitor your credit.** This will not prevent any fraud, but it may help you catch any theft of your identity before it gets too bad. There are a number of ways to monitor your information.
   a. Check for free credit monitoring. Agencies, such as, Equifax, TransUnion or Experian offer free credit monitoring. You get free access to your report once a year for each of the three bureaus. We recommend getting a report from one bureau every four months and alternating. Free is good, but it can be hard for you to remember to do this regularly, and you may not want to let four months go by without monitoring.
   b. Pay a third-party service. Typically, you'll pay around $10-$20 monthly for a high-quality service. These services will monitor all three credit bureaus and notify you of any changes. There are also additional protections offered, such as insurance that covers you for id-theft-related losses.
   c. *Go to annualcreditreport.com to periodically check your reports for yourself.*

2. **Set up fraud alerts with the credit bureaus.**
   a. An Initial Security Alert if you suspect you are a victim of identity theft. This adds a message to your credit report for 90 days, notifying creditors that they should take extra precaution to ensure that they are talking to the real you. Once you do this with any of the credit bureaus, they will notify and add the alert at the other bureaus for you.
   b. An Extended Security Alert, if you have a police report. This stays on file for up to 7 years, and requires creditors to contact you at a preapproved phone number before extending credit.
   c. You can also add fraud alerts with credit card companies, though most major credit card companies already monitor your accounts for suspicious activity.

3. **Freeze your credit reports with all three bureaus.** This is the most extreme step you can take, but it is also the most secure. You will be provided with a PIN, which you must provide to the bureau to temporarily "thaw" your report any time somebody needs to access it legitimately.
   a. Depending on the state you live in, there may be a small cost to freeze your credit – typically $3-$10. If you live in North Carolina, a freeze can be done for free at: http://www.ncdoj.gov/freefreeze
   b. The freeze remains in place permanently, though you can permanently remove it at any time. *Note, a freeze is automatically ended after 7 years if you live in a handful of states (but not NC).

4. **Do NOT give your Social Security number or other personal information to anybody who emails or calls you.** It seems inevitable that opportunistic criminals will start making calls claiming to be from a reporting agency and offering to "help protect you". If this happens, hang up immediately and notify the Federal Trade Commission using their Complaint Assistant Site:

   www.ftccomplaintassistant.gov

5. **Help protect your loved ones** who might be especially vulnerable, like young adults and senior citizens. Educate and remind them not to provide their personal information to anybody who calls or emails them. Be aware that the credit bureaus are handling a tremendous deal of phone and web traffic right now. If you call, expect a long wait time. And if you get an error message for an online credit freeze or fraud alert, you may have to wait a few days and try again. Unfortunately, the technology that makes our world better also creates new opportunities for criminals, so you have to protect yourself. Finally, we apologize again for the inconvenience this has caused you. Feel free to contact us at the information listed above if you have any questions or need any assistance understanding this matter.

Best Regards,

Accurate Word, LLC

September __, 2019