May 29, 2018

VIA FEDERAL EXPRESS

Office of the Attorney General
Consumer Protection and Antitrust Bureau
33 Capital Street
Concord, NH 03301

Dear Sir or Madam:

PrintingCenterUSA.com recently learned of a computer data security incident that potentially affects customers who made purchases through our website, www.printingcenterUSA.com, or our call center, from January 2018 to May 9, 2018. We have found no evidence that the incident resulted in the unauthorized access or acquisition of customer information. Out of an abundance of caution, however, PrintingCenterUSA.com is voluntarily providing notification of the potential incident to any customers who made purchases from January 2018 to May 9, 2018.

During recent review of our website and systems we discovered some suspicious code that may have been present on our website at times from January 2018 through May 9, 2018. We believe that this code was a result of activity relating to one of our vendors. This code may have had the ability to capture some customer account logon and payment card information as it was entered by customers into our website forms and shopping pages, but before PrintingCenterUSA.com received it on our systems.

We have no indication that customer account logon and payment card information was accessed, acquired, or misused. Also, we only collect limited information from our customers, including first and last name, email address and password, address, payment card number(s) with expiration date(s), and phone number. We also encrypt payment card information and have no evidence that an encryption key was compromised.

We are notifying 5 individuals with billing addresses in New Hampshire who may have made purchases through www.printingcenterUSA.com, or our call center, from January 2018 to May 9, 2018.

As a courtesy to our customers, PrintingCenterUSA.com began to voluntarily notify those customers on May 25, 2018, and offer our valued customers one year of free credit monitoring services through Kroll Associates, Inc. A sample of this voluntary disclosure letter is enclosed as Exhibit A.

While our investigation continues, we are working with a leading cybersecurity firm to remove any known suspicious code, make security updates, strengthen access controls,

force password changes, vendor review, and continue to monitor our systems. Our work is still ongoing and we are working with legal counsel on the matter.

As your office may hear about this incident, we deemed it prudent to inform you about the steps that PrintingCenterUSA.com is taking to protect and assist its customers located in your state. Thus, as a courtesy, we are voluntarily providing this notice to you in the interest of keeping you fully informed.

Please feel free to contact me with any questions at kevans@printingcenterusa.com or (800) 995-1555 ext. 102.

Sincerely,

Kevin Evans
Account Services Director
PrintingCenterUSA.com
117 9th Street N.
Great Falls, MT 59401

EXHIBIT A

PrintingCenterUSA.com

[redacted]

[redacted]

Dear [redacted],

Thank you for being a loyal PrintingCenterUSA.com customer. We are writing about certain account logon and payment card transaction information ("Information") associated with purchase(s) made through our website www.printingcenterUSA.com, or our call center, including purchases you may have made with the following card(s): [redacted]

Although we have no evidence of any breach of our systems or actual misuse of the Information provided by you or any of our customers, we are voluntarily providing this information to you as a courtesy in the interest of keeping you fully informed.

What Happened?

We reviewed our website and systems and discovered some suspicious code that may have been present on our website at times from January 2018 through May 9, 2018. We believe that this code was a result of activity relating to one of our vendors. This code may have had the ability to capture Information as it was entered by customers into our website forms and shopping pages, but before we had received it on our systems. We found no evidence that the code resulted in the unauthorized access or acquisition of customer Information.

What Information Was Involved?

While we have no indication that any customer Information was acquired or misused, you may recall from shopping on our website or ordering through our call center that customers are required to enter certain limited Information:

- first and last name
- address
- phone number
- account email address and password
- payment card number(s) with expiration date(s)

Note, we store payment card numbers in an encrypted manner and there is no evidence that any encryption or encryption key was compromised.

What We Are Doing.

While our investigation continues, we are working with a leading cybersecurity firm to remove any known suspicious code, make security updates, strengthen access controls, force password changes, conduct vendor review, and continue to monitor our systems.

What You Can Do.

We are unaware of any of our systems being accessed and do not know of any actual misuse of Information associated with this matter. However, consumers should regularly and vigilantly review their payment card statements and report any suspicious activity to their card issuer. You may also contact your card company and inform them of this matter and ask to have a new card number issued, change account log in credentials, and use different and strong passwords on all of your accounts.

In addition, if it provides comfort to you, as a courtesy and in recognition for how much we value your business, we are offering free credit monitoring services to customers receiving this notification. We have arranged with Kroll to offer you the option of one year of credit monitoring at no cost to you. If you would like to take advantage of this offer, **you must enroll by August 23, 2018**. You can activate your membership by visiting Kroll's website at [redacted] To receive credit services by mail, please call [redacted] Please reference your membership number: [redacted]. Also, please refer to the attached document from Kroll, which provides an overview of the services available to you.

For More Information.

For information about credit monitoring and the security of information, please contact Kroll at [redacted] Monday through Friday between 8:00 a.m. and 5:00 p.m. Central Standard Time.

We apologize for any inconvenience this incident may cause you. We value your business.

Sincerely,

Craig Barber
President

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies is:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual 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 from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. 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.

Security Freeze. You have the ability 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 may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. 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 credit reporting agencies may charge a fee to place a freeze, temporarily lift it or permanently remove it. The fee is waived if you are a victim of identity theft and have submitted a valid investigative or law enforcement report or complaint relating to the identity theft incident to the credit reporting agencies. (You must review your state's requirement(s) and/or credit bureau requirement(s) for the specific document(s) to be submitted.)

For Massachusetts residents: The fee for each placement of a freeze, temporary lift of a freeze, or removal of a freeze is $5.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

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

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and 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.