BakerHostetler

Baker&Hostetler LLP
11601 Wilshire Boulevard
Suite 1400
Los Angeles, CA 90025-0509
T 310.820.8800
F 310.820.8859
www.bakerlaw.com

April 5, 2016

M. Scott Koller
direct dial: 310.979.8427
mskoller@bakerlaw.com

VIA OVERNIGHT DELIVERY

Office of the Attorney General
Consumer Protection Division
Hoover State Office Building
1305 E. Walnut St.
Des Moines, IA 50319

Re: Incident Notification

Dear Sir or Madam:

Our client, Katherman Kitts & Co. LLP, ("KKC"), learned on February 25, 2016, that hard drives containing backup files for one of the firm's servers, along with other incidental items, were stolen from a partner's locked vehicle. KKC immediately notified the Long Beach Police Department and began a thorough investigation to determine what information was contained on the hard drive.

After a detailed review, KKC confirmed that the hard drives may have contained files with differing amounts of employee and client information, including name, address, date of birth, driver's license number, Social Security number, and other information typically included in tax returns.

KKC has no reason to believe that the drives were stolen for the information they contained or that the information has been accessed or used in any way. Although the drives were not encrypted, there is nothing on the exterior of the drives to indicate what is on them and KKC has consulted a technology expert who has confirmed it would take a fairly sophisticated criminal with technical expertise to access the information. Still, as a precaution, KKC began notifying affected individuals in person and over the phone on March 1, 2016 with written notification on April 5, 2016. KKC is offering affected individuals one year of complimentary credit monitoring and identity theft protection services through AllClear.

KKC is notifying seven (7) Iowa residents in substantially the same form as the letters attached hereto.[1] Notification is being provided in the most expedient time possible and without unreasonable delay pursuant to the investigation described above, which was necessary to determine the scope of the incident; restore the reasonable integrity of the data system; and identify the individuals potentially affected. *See* IOWA CODE ANN. § 715C.2(1).

To prevent this from happening again, KKC re-enforcing education and training for all employees regarding the importance of handling information securely and is implementing additional technical safeguards to protect personal information.

[1] This report is not, and does not constitute, a waiver of personal jurisdiction.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

M. Scott Koller

M. Scott Koller

Enclosures

Katherman Kitts & Co. LLP
Certified Public Accountants and Business Advisors

Processing Center • P.O. Box 141578 • Austin, TX 78714

00001
00001
ACD1234
JOHN Q. SAMPLE
1234 Main Street
Anytown US 12345-6789

April 5, 2016

NOTICE OF DATA BREACH

Dear John Sample:

As a most valued client of our firm, I am writing to let you know of an unfortunate incident that recently took place and the measures we are taking to minimize risk of any negative consequences.

What Happened?
On February 25, 2016, hard drives containing backup files for one of the firm's servers, along with other incidental items, were stolen from a partner's locked vehicle. These files may have contained some of your confidential information as a client of Katherman Kitts & Co. LLP. The partner discovered the theft later that evening and immediately notified the Long Beach Police Department. We are continuing to work with law enforcement to locate the stolen hard drives.

What Information Was Involved?
The information stored on the hard drives may include your name, address, date of birth, Social Security number, and other information typcially included in your tax return.

What We Are Doing.
We have no reason to believe that the drives were stolen for the information they contained or that the information has been accessed or used in any way. There is nothing on the exterior of the drives to indicate what is on them and we have consulted a technology expert who has confirmed it would take a fairly sophisticated criminal with technical expertise to access the information. In addition, our private investigator told us the theft had all the markings of a random event, likely carried out by local teenagers because other cars were also broken into and stolen credit cards were immediately used to purchase video games and movie rentals. Nevertheless we are taking no chances and have taken steps to closely monitor the situation and to mitigate risk of client information exposure by arranging for AllClear ID to 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 SECURE: The team at AllClear ID is ready and standing by if you need identity repair assistance. This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-865-4458 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear PRO: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. For a child under 18 years old, AllClear ID ChildScan identifies acts of credit, criminal, medical or employment fraud against children by searching thousands of public databases for use of your child's information. To use the PRO service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-865-4458 using the following redemption code: Redemption Code. Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

We have taken steps to thoroughly review all of our security protocols to make sure they are clear, unambiguous and understood by everyone in our office. We are re-enforcing education and training for our employees regarding the importance of handling information securely and are implementing additional technical safeguards to protect information in our care. We are confident we have taken the correct steps to ensure that a similar incident will not happen in the future.

What You Can Do.
We encourage you to take advantage of the identity theft protection services being offered. Further, you should remain vigilant to the possibility of fraud and identity theft by reviewing credit card, bank, and other financial statements for any unauthorized activity.

For More Information.
Protecting your information is incredibly important to us, as is addressing this incident with the information and assistance you may need. If you have any questions or concerns, please call us at 1-855-865-4458.

Thank you for your understanding and continued support. We are deeply grateful.

Sincerely,

Katherman Kitts & Co LLP

Katherman, Kitts & Co., LLP
Stacie Kitts, Managing Partner

Information about Identity Theft Protection

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax, P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com
Experian, P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion, P.O. Box 1000, Chester, PA 19016, 1-877-322-8228, www.transunion.com

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the toll-free numbers listed below:

Equifax	Experian	TransUnion
877-478-7625	888-397-3742	800-680-7289

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

Equifax Security Freeze	Experian Security Freeze	TransUnion (FVAD)
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	freeze.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

AllClear Secure 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 Secure 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 Secure 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 that occurred prior to your Coverage Period are not covered by AllClear Secure services.

Eligibility Requirements
To be eligible for Services under AllClear Secure 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 Secure services (an "Event"), 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 Secure 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 Secure 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 Secure 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 Secure 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 Secure 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 Secure, please contact AllClear ID:

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