Joshua James
Associate
Direct: 202/508-6265
Josh.James@BryanCave.com

June 27, 2014

CONFIDENTIAL

VIA FEDERAL EXPRESS

Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Data Security Breach Voluntary Notification

To Whom It May Concern:

Benjamin F. Edwards & Co ("BFE"), a client of Bryan Cave LLP, is voluntarily notifying the office of the attorney general that BFE intends to notify 430 residents of New Hampshire of a malware incident. This letter is being provided as a courtesy as we do not believe notification is required under N.H. Rev. Stat. Ann. § 359-C:19.

On May 27, 2014, BFE discovered that it was a victim of an unauthorized attempt to access its electronic data. Based on its investigation, BFE believes that some of its information was taken; however, it is not possible to determine specifically what that information included. BFE does not have specific evidence that sensitive personal information about New Hampshire residents was acquired by a third party.

In more detail, an employee of BFE was the victim of a CryptoWall malware infection (a variant of the more common CryptoLocker malware) that encrypted files on the employee's computer and files on certain shared drives to which the user had access. As a result of the infection, data was transferred to a suspicious IP address. The investigation of a professional forensic expert has not, however, been able to reveal the content of the data transmitted to the IP address.

After BFE became aware of the incident it took immediate steps to remove the malware and consulted with a computer forensics specialist to help in its investigation. BFE also notified law enforcement, the Financial Industry Regulatory Authority ("FINRA"), and the Missouri Securities Commissioner regarding the incident.

Since this incident occurred, BFE has, among other things, further restricted the IP addresses which can be visited by BFE employees and supplemented its security infrastructure with additional devices and practices that may help prevent CryptoWall attacks in the future.

Although we have no specific evidence that a New Hampshire resident's data was actually acquired or accessed by a third party, out of an abundance of caution BFE is sending a notification letter to every current and former client and employee who BFE knew to reside in New Hampshire (430 individuals) via US mail on, or around, June 27th. A sample of the notification letter is attached. As you can see, each individual will be provided one year of free credit monitoring, identity theft protection, and fraud resolution services through AllClear ID.

If you would like any additional information concerning the above event, please feel free to contact me at your convenience.

Sincerely,

Joshua James

Enclosure

ENCLOSURE

BENJAMIN F. EDWARDS & CO.

Benjamin F. Edwards & Co. c/o AllClear ID, Inc.
PO Box 3825
Suwanee, GA 30024

June 27, 2014

40 1 9741 **********AUTO**3-DIGIT 082
John Q Sample
123 Any Street
Anytown, US 12345-6789

Dear John Q Sample,

We strongly value the trust you have placed in your relationship with Benjamin F. Edwards & Co. (BFE). We also know that you expect your personal information to be secure and protected, and we take our responsibility in this regard very seriously. That is why we are writing to you.

On May 27, 2014, BFE discovered, like many other businesses and financial institutions, that it was a victim of an unauthorized attempt to access our electronic data. Based on the results of our investigation, we have learned some of our information was taken; however, we do not have any specific evidence that your information was acquired by a third party or has been fraudulently used. Nonetheless, because those possibilities exist, we are voluntarily providing you with information regarding this incident to demonstrate that your security, and your trust, are an absolute priority for us.

After discovering the incident, we immediately took action to terminate the attack and consulted with a third party computer forensics specialist to help in our investigation. We also notified law enforcement and industry regulators and have expressed our willingness to cooperate in any investigation they undertake. We have also taken additional proactive security measures to help prevent a similar incident from occurring in the future; however, due to the nature of cybersecurity attacks, it is virtually impossible to entirely prevent these types of events from ever occurring.

It is always a good practice to monitor all of your financial accounts for any signs of suspicious activity. Also, if you determine that an account has been fraudulently established using your identity, you should call a credit reporting agency immediately as well as contact the Federal Trade Commission and your state attorney general. Contact information, along with instructions on how to obtain more information about identity theft, are included in an attachment to this letter. You should also consider changing various online passwords.

As a precaution, we are offering identity protection, credit monitoring and fraud assistance services from AllClear ID for 12 months at no cost to you. These services start on June 27, 2014 and will be available at any time during the next 12 months:

AllClear SECURE: This service provides individuals with a trained representative to assist them in the event they experience a fraud-related issue resulting from this incident. Affected individuals are automatically eligible to use this service – there is no action required on their part to enroll. You can access the service by calling (toll free) or + (toll).

AllClear PRO: This service offers credit monitoring and identity theft insurance. Beginning on June 27, 2014, please call . (toll free) or (toll), or log on to www.enroll.allclearid.com to learn more and sign up for these services using the following redemption code:

We thank you for your continued confidence in BFE, and sincerely apologize for any inconvenience you may experience as a result of this incident. We invite our current clients and employees to contact their Financial Consultant, and our former clients and employees to call . toll free) or (toll) regarding this matter or the protections available to you.

Sincerely,

Albert J. Tylka, Jr.
Director of Operations

ADDITIONAL ACTIONS TO HELP REDUCE YOUR CHANCES OF IDENTITY THEFT

Information about reporting and preventing identity theft can be found at http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/index.html. Among other things, this website explains how to ask the national credit reporting agencies to place a "fraud alert" or a "security freeze" on your credit reports. A fraud alert is a statement added to your credit report that alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. A security freeze is a statement added to your credit report that alerts creditors not to open accounts under your name. If you have been a victim of identity theft and provide a credit reporting agency with a valid police report, they will not charge you to place, lift, or remove a security freeze. In other cases, a credit reporting agency may charge a small fee (typically no more than $10, although the fee varies by state; in Massachusetts the fee is $5) to place, lift or remove a security freeze. The following is the contact information for the three national credit reporting agencies:

COMPANY	TELEPHONE	ADDRESS	WEBSITE
Equifax	800-525-6285	P.O. Box 740241 Atlanta, GA 30374-0241	http://www.equifax.com
Experian	888-397-3742	P.O. Box 9532 Allen, TX 75013	http://www.experian.com
TransUnion	800-680-7289	Fraud Victim Assistance Division P.O. Box 6790 Fullerton, CA 92834-6790	http://www.transunion.com

In addition, if you are a victim of identity theft, you have the right to file a police report regarding that identity theft and obtain a copy of your police report. You also should consider reporting the incident to the Federal Trade Commission. They can be reached at 1-877-438-4338, Federal Trade Commission, Bureau of Consumer Protection, 600 Pennsylvania Avenue, NW Washington, DC 20580, or online at https://www.ftccomplaintassistant.gov/. You should also consider contacting your state's Attorney General and/or Division of Consumer Protection to report ID theft or for more information about ID theft. If you are a resident of Maryland or North Carolina, you can obtain additional information for how to avoid identity theft (including how to place a fraud alert or security freeze on your account) and how to report identity theft from the following sources:

MD Attorney General's Office Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us	NC Attorney General's Office Consumer Protection Division 9001 Mail Service Center Raleigh, NC 27699-9001 1-877-566-7226 http://www.ncdoj.gov/

AllClear Secure Terms of Use

- Automatic 12 months of coverage
- 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
You are automatically protected for 12 months from the date the breach incident occurred, as communicated in the breach notification letter 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, reside in the United States, 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, you must:

- Notify AllClear ID by calling 1.855.434.8075 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;
- 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
    - 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;
- 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; and
- 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;
- You are expected to protect your personal information in a reasonable way at all times. Accordingly, you will not recklessly disclose or publish your Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information, such as, by way of example, in response to "phishing" scams, unsolicited emails, or pop-up messages seeking disclosure of 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