STEARNS WEAVER MILLER
WEISSLER ALHADEFF & SITTERSON, P.A.

Kelly R. Melchiorido
150 West Flagler Street, Suite 2200
Miami, FL 33130
Direct: (305) 789-3529
Fax: (305) 789-2640
Email: kmelchiondo@stearnsweaver.com

July 3, 2019

Via Certified Mail

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

Re: Report of Data Security Incident

Dear Attorney General MacDonald:

We are counsel to BBX Capital Corporation, which is headquartered in Ft. Lauderdale, Florida. We write to notify your office of a security incident that may have exposed the Personal Information, including names, addresses, Social Security numbers, and financial account information, of one (1) New Hampshire resident.

On March 27, 2019, suspicious emails that attached malware and malicious code were sent using BBX Capital employee email accounts. BBX's preliminary investigation revealed several unauthorized logons or attempted logons into BBX email accounts by an unauthorized user, beginning on March 26, 2019. On March 28, 2019, the unauthorized user either logged in, or attempted to log in, to additional BBX email accounts. On March 28, 2019, BBX changed all employee passwords to prevent the unauthorized user from any further access to BBX's network and email accounts.

On April 2, 2019, BBX hired a forensic data consultant to conduct a thorough investigation of the security incident. On April 30, 2019, the forensic consultant advised BBX that several BBX employee email accounts had been compromised, and that compromised accounts contained Personal Information in emails. BBX's forensic consultant could not determine whether the unauthorized user had accessed or removed any Personal Information from the employees' emails.

On May 1, 2019, BBX hired a second forensic consultant to determine whether the unauthorized user had accessed Personal Information in the employee emails. The second

forensic consultant advised BBX on May 16, 2019 that it also could not determine whether the unauthorized user had accessed Personal Information from the emails.

While BBX does not believe that it is likely that the unauthorized user obtained or removed any Personal Information from BBX's emails or network, BBX has chosen to report this security incident to all persons whose Personal Information was potentially exposed in an abundance of caution. BBX will notify the New Hampshire resident and will offer him or her free credit monitoring and identity theft services through Kroll Information Assurance, LLC, for a period of twelve (12) months. A sample of the notification letter is enclosed for your review.

From May 17, 2019 through June 15, 2019, BBX conducted a thorough review of all Personal Information electronically stored in the affected employees' emails. BBX confirmed on June 15, 2019 that the New Hampshire resident's Personal Information may have been exposed because his or her name, address, Social Security Number and/or financial account information was contained in the affected employees' emails.

If you would like additional information regarding this matter, please feel free to contact me at your convenience.

Sincerely,

Kelly R. Melchiondo

KRM: eg
Enclosures

BBX Capital

<<Date>> (Format: Month Day, Year)

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

RE: Important Security Notification
Please read this entire letter.

Dear Mr. or Ms. <<Last Name>>:

On March 27, 2019, suspicious emails were sent from BBX Capital employee email accounts. The suspicious emails attached files that contained malware and malicious code. BBX's preliminary investigation revealed several unauthorized logons or attempted logons into BBX email accounts from an unauthorized user, beginning on March 26, 2019. On March 28, 2019, the unauthorized user either logged in, or attempted to log in, to additional BBX email accounts. On March 28, 2019, BBX changed all employee passwords and prevented the unauthorized user from any further access to BBX's network and email accounts.

On April 2, 2019, BBX hired a forensic data consultant to conduct a thorough investigation of the security incident. On April 30, 2019, the forensic consultant advised BBX that several BBX employee email accounts had been compromised, and that compromised accounts contained Personal Information in emails. BBX's forensic consultant could not determine whether the unauthorized user had accessed any Personal Information in the employees' emails.

On May 1, 2019, BBX hired a second forensic consultant to determine whether the unauthorized user had accessed Personal Information in the employee emails. The second forensic consultant advised BBX on May 16, 2019 that it could not determine whether the unauthorized user had accessed Personal Information from the emails.

Therefore, while BBX has no reason to believe that the unauthorized user accessed, obtained or used your Personal Information, BBX nonetheless wants to make you aware of the security incident as a precaution.

Because data privacy and your privacy are paramount to BBX, BBX has opted to identify and notify all persons whose Personal Information may have been exposed during the March 26-28, 2019 security incident. From May 17, 2019 through June 15, 2019, BBX conducted a thorough review of the Personal Information stored in the employee emails. BBX confirmed on June 15, 2019 that your Personal Information was included in the employee emails.

To address this incident, BBX has secured the services of Kroll to provide identity monitoring at no cost to you for **twelve (12) months**. The identity monitoring services that Kroll will provide to you include Credit Monitoring, a Current Credit Report, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration. We enclose a description of Kroll's services.

Visit **<<IDMonitoringURL>>** to activate and take advantage of your identity monitoring services.
*You have until **<<Date>>** to activate your identity monitoring services.*
Membership Number: **<<Member ID>>**

BBX encourages you to review the Additional information that describes Kroll's services and is included with this letter.

BBX encourages you to review the "Additional Resources" document enclosed here. That document describes additional steps that you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

If you have questions, please call 1-???-???-????, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. Please have your membership number ready.

While BBX does not believe that the security incident exposed your Personal Information, BBX sincerely apologizes for any inconvenience this may cause you. We encourage you to take advantage of the identity monitoring services we have offered through Kroll.

Sincerely,

Kirsten Uebrig
BBX Capital Corporation

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.

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.

Kroll. | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

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

Triple Bureau Credit Monitoring and Single Bureau Credit Report

Your current credit report is available for you to review. You will also receive alerts when there are changes to your credit data at any of the three national credit bureaus—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.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You'll receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

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.