

STATE OF NH
DEPT OF JUSTICE

2015 APR -2 AM 9:47

[REDACTED]

April 1, 2015

**CONTAINS CONFIDENTIAL INFORMATION
VIA OVERNIGHT DELIVERY**

Attorney General Joseph Foster
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Security Incident Involving Retail Capital, LLC

Dear Attorney General Foster:

This firm represents Retail Capital, LLC ("Retail Capital"). Pursuant to New Hampshire Rev. Stat. Ann. § 359-C:20(l)(b), this letter is to inform you of a data security incident involving a single user email box of a Retail Capital employee that occurred on March 17, 2015. Retail Capital identified the intrusion, re-established the security of the compromised electronic mailbox within approximately 40 minutes and immediately initiated an investigation.

Retail Capital provides growth capital to help small businesses expand, purchase inventory or equipment, or manage working capital. Retail Capital is headquartered in Troy, Michigan. The company was formed in 2010 and currently employs 75 people (full-time-equivalents) in Troy and its other office locations.

The incident involved unauthorized access by an unidentified third party to the electronic mailbox of one of Retail Capital's sales managers. The mailbox contained funding applications and supporting information submitted by small businesses (including sole proprietorships) seeking to use Retail Capital's services. Thus, although personal information was included with the applications, including one or more of individual principals' names, addresses, Social Security numbers, driver's license numbers and bank account numbers or statements, the individuals were interacting with Retail Capital in business, not consumer, capacities. At this time we believe that information concerning **3 New Hampshire residents** (out of a total of 741 notified data subjects) was contained in the mailbox. Those residents are being notified by mail on April 2, 2015, and a copy of that notice is enclosed.

The intruder was able illicitly to acquire the manager's password, thereby gaining access to the manager's electronic mailbox. Upon gaining access, the intruder locked Retail Capital's employee out of the mailbox. Retail Capital does not believe any other employee mailbox or system resource was compromised. Retail Capital became aware of the intrusion almost immediately and was able to lock out the intruder within 40 minutes of the intrusion. The company has no reason to believe any specific person's personal information was accessed or otherwise compromised, but, because the mailbox contained personal information, is providing notice.

Retail Capital understands the importance of its applicants' personal and business information. The company takes very seriously its obligation to safeguard that information and to use it in an appropriate manner. Retail Capital has implemented additional security procedures that are intended to prevent recurrence of this or a similar type of event, including a new access procedure for all employees. Employees now must utilize dual-factor authentication (currently, Google's Authenticator tool which

[REDACTED]

PAUL
HASTINGS

Office of the Attorney General
April 1, 2015
Page 2

requires both a password and a code sent to the employee's phone via text, voice call or Google's mobile app) in order to access their mailboxes.

As a cautionary measure, to protect against any potential misuse of information that may result from the compromise, Retail Capital will offer affected individuals **identity theft coverage for a period of two years** through ID Experts. ID Experts®, data breach and recovery services expert, will provide fully managed recovery services which include: 2 years of FraudStop™ credit monitoring, a \$20,000 insurance reimbursement policy, exclusive educational materials and complete access to their fraud resolution representatives.

Should you have any questions or concerns regarding this matter, please contact me for additional information.



Enclosure



RetailCapital

Fast. Easy. Flexible.

Retail Capital
C/O ID Experts
10300 SW Greenburg Road, Ste 570
Portland, OR 97223

[Name]
[Address1]
[Address2]
[City, State Zip]

Date

Dear Current or Former Applicant:

We write to you with important information about a potential compromise of certain personal information that occurred on March 17, 2015. The incident involved unauthorized access by an unidentified third party to the electronic mailbox of one of our sales managers. The intruder was able illicitly to acquire the manager's password, thereby gaining access to the manager's electronic mailbox. Upon gaining access, the intruder locked our employee out of the mailbox. We identified the intrusion and re-established the security of the mailbox within approximately 40 minutes. We do not believe any other employee mailbox or system resource was compromised. We also have implemented additional security procedures that are intended to prevent recurrence of this or a similar type of event.

As noted, the intrusion lasted only about 40 minutes, and we have no specific basis to conclude that your personal information was accessed. Nonetheless, our sales manager's mailbox contained funding applications and related information provided by applicants in support of their applications, including one or more of your name, business address, Social Security number, driver's license number and bank account number or statements. For that reason, we provide you with this notice.

In an effort to protect against any potential misuse of information that may result from the compromise, **Retail Capital will provide you identity theft coverage for a period of two years through ID Experts.** ID Experts®, data breach and recovery services expert, will provide you with fully managed recovery services which also include: 2 years of FraudStop™ credit monitoring, a \$20,000 insurance reimbursement policy, exclusive educational materials, and complete access to their fraud resolution representatives. With this protection, ID Experts will help you resolve issues if your identity is compromised.

We encourage you to contact ID Experts with any questions and to enroll in the free services by calling 1-888-653-7709 or going to www.idexpertscorp.com/protect. ID Experts is available by phone Monday through Friday from 9 am - 9 pm Eastern Time through May 1, 2015. Online enrollment will be available through July 1, 2015. **Your Access Code is:**

We also recommend that you contact your bank and any credit card companies immediately to notify them of the potential disclosure of your Social Security number. Going forward, you should continue to monitor your account statements for evidence of fraud. You also may take the following precautions to safeguard your personal information:

- Call the toll-free numbers of any one of the three major credit bureaus to place a fraud alert on your credit report. This can help prevent an identity thief from opening additional accounts in your name. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place alerts on your credit report, and all three reports will be sent to you free of charge.
 - **Equifax:** 1-888-766-0008
https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp; Equifax Consumer Fraud Division, PO Box 740256, Atlanta, GA 30374
 - **Experian:** 1-888-397-3742; www.experian.com; Experian Fraud Division, P.O. Box 9530, Allen, TX 75013
 - **TransUnion:** 1-800-680-7289; www.transunion.com; TransUnion Fraud Victim Assistance Department, P.O. Box 2000, Chester, PA 19022
- Order your credit reports. By establishing a fraud alert, you will receive a follow-up letter that will explain how you can receive a free copy of your credit report. When you receive your credit report, examine it closely and look for signs of fraud, such as credit accounts that are not yours.
- Call the Federal Trade Commission (FTC) to get more information about fraud and identity theft. The FTC operates a call center for identity theft victims where counselors tell consumers how to protect themselves and what steps to take if they become victims of identity theft.
 - **Federal Trade Commission:** 1-877-IDTHEFT (1-877-438-4338); www.ftc.gov/idtheft; 600 Pennsylvania Avenue, NW, Washington, DC 20580
- Consider placing a security freeze on your credit reports. Unlike a fraud alert, which is free and alerts creditors to employ heightened identity verification before extending new or additional credit in your name, a security freeze restricts the credit bureaus' ability to release your credit information to third parties without your permission. Security freezes are not available in every state, and may incur an additional charge.

Please contact us at 1-888-653-7709 for additional information, or we encourage you to enroll online at www.idexpertscorp.com/protect.

Retail Capital understands the importance of your personal and business information. We take very seriously our obligation to safeguard that information and to use it in an appropriate manner. We deeply regret this occurrence and hope that it has not damaged your confidence in

us. Retail Capital continually assesses our security measures to explore ways in which we might protect and improve the security of the information we maintain. This incident only serves to reinforce that commitment.

Sincerely,

Glenn Goldman
Chief Executive Officer, Retail Capital LLC

ID Experts Recommended Steps for Enrollment and Protecting Your Information

1. Website and Enrollment: Go to www.idexpertscorp.com/protect and follow the instructions for enrollment using your Access Code provided above. Once you have completed your enrollment, you will receive a welcome letter by email (or by mail if you do not provide an email address when you sign up). The welcome letter will direct you to the exclusive ID Experts' Member Website where you will find other valuable educational information.

2. Activate the credit monitoring provided as part of your membership with ID Experts, which is paid for by Retail Capital. Credit monitoring is included in the membership, but you must personally activate it for it to be effective. Please note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, ID Experts will be happy to help you.

3. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.privacy.ca.gov) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118, Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.com/, Telephone: 1-919-716-6400.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TDD: 1-202-326-2502.