



55 East Monroe Street  
37th Floor  
Chicago, IL 60603

312 346 7500 main  
312 580 2201 fax  
thompsoncoburn.com

**Melissa K. Ventrone**  
312 580 2219 direct  
mventrone@thompsoncoburn.com

May 10, 2017

**Attorney General Joseph Foster**  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03302

**RECEIVED**

**MAY 15 2017**

**CONSUMER PROTECTION**

Dear Attorney General Foster:

We represent Capital First Trust Company ("Capital First") with respect to a recent security incident involving the potential exposure of certain personally identifiable information described in more detail below. Capital First is a company based in Milwaukee, Wisconsin, and provides services related to financial trusts.

**1. Nature of security incident.**

On March 7, 2017 one of Capital First's trust investment advisors informed Capital First that it had detected suspicious activity related to Capital First's online accounts. Capital First began an internal investigation and hired an independent computer forensics company to assist. On April 7, 2017, the computer forensic company informed Capital First that an unauthorized user had gained access to two Capital First user accounts. This access was limited to these users' email accounts and shared files. After reviewing the email accounts and shared files, Capital First determined that information related to a limited number Capital First's clients or employees may have been at risk. This information included names, addresses, account numbers, driver's license number, and Social Security numbers.

**2. Number of New Hampshire residents affected.**

Capital First identified records for one (1) New Hampshire resident impacted as a result of this incident. A notification letter was mailed to the individual on May 10, 2017 via regular mail. Enclosed please find a copy of the notification letter.

**3. Steps you have taken or plan to take relating to the incident.**

Capital First is working with the computer forensics company to further enhance the security of its systems. Capital First has already take steps to enhance the security of information in its system, including adding new, stronger password and encryption measures to its systems. Finally, Capital First has offered 12 months of credit monitoring and identity theft protection through Kroll to its clients at no cost.

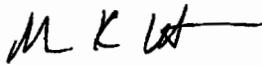
May 10, 2017  
Page 2

**4. Contact information.**

Capital First remains dedicated to protecting the sensitive information in its systems. If you have any questions or need additional information, please do not hesitate to contact me at [MVentrone@ThompsonCoburn.com](mailto:MVentrone@ThompsonCoburn.com) or (312) 580-2219.

Very truly yours,

Thompson Coburn LLP

A handwritten signature in black ink, appearing to read "M K Ventrone", with a long horizontal flourish extending to the right.

Melissa K. Ventrone

Enclosures



<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Date>> (Format: Month Day, Year)  
<<Address1>>  
<<Address2>>  
<<City>>, <<State>> <<ZipCode>>

### Notice of Data Security Incident

Dear <<MemberFirstName>> <<MemberLastName>>,

We are writing to inform you about a data security incident experienced by Capital First Trust Company (“Capital First”) that may have exposed your personal information, including your name and Social Security number. Capital First was in possession of your personal information because we are the named trustee for a trust with which you are associated. We value and respect the privacy of your information, and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information, and resources we are making available to help you.

#### 1. What happened and what information was involved?

On March 7, 2017 one of Capital First’s trust investment advisors informed Capital First that they had detected suspicious activity related to Capital First’s online accounts. Capital First began an internal investigation and hired an independent computer forensics company to assist. On April 7, 2017, the computer forensic company informed Capital First that an unauthorized user had gained access to two Capital First user accounts, which was limited to these users’ email accounts and shared files. From our review, the email accounts or shared files may have contained information related to your accounts with us, such as your name, address, Social Security number, driver’s license number, credit card number, or your bank account information.

#### 2. What we are doing and what you can do.

While we do not have any indication that your information has been misused, we have arranged for you to receive identity monitoring services from Kroll at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. We recommend you respond promptly to any indications of identity theft, and utilize Kroll’s services. Your identity monitoring includes Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit [krollbreach.idMonitoringService.com](http://krollbreach.idMonitoringService.com) to activate and take advantage of your identity monitoring services.

*You have until August 10, 2017 to activate your identity monitoring services.*

Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-844-263-8605.

We also recommend you remain vigilant over the next 12 to 24 months and monitor your accounts for any suspicious activity. Please review the enclosed additional information section included with this letter. This section describes additional steps 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.

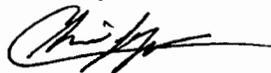
We want to assure you that we are taking steps to prevent this sort of incident from occurring in the future. We are working with the computer forensics company to further enhance the security of our systems. Additionally,

we have taken steps to enhance the security of information in our system, such as adding new, stronger password and encryption measures to our systems.

**3. For more information.**

If you have questions, please call 1-866-775-4209, Monday through Friday from 8:00 a.m. to 5:00 p.m. Central Time. Please have your membership number ready. Your trust is a top priority for us, and we deeply regret any inconvenience or concern this matter may cause you.

Sincerely,



Chris Foregger  
President and COO  
Capital First Trust Company

## U.S. State Notification Requirements

---

### For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina:

It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

---

### For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia:

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report by contacting any one or more of the following national consumer reporting agencies:

<b>Equifax</b> P.O. Box 105139 Atlanta, GA 30374 1-800-685-1111 www.equifax.com	<b>Experian</b> P.O. Box 2002 Allen, TX 75013 1-888-397-3742 www.experian.com	<b>TransUnion</b> P.O. Box 6790 Fullerton, CA 92834 1-800-916-8800 www.transunion.com
---	---	---

You may also obtain a free copy of your credit report online at [www.annualcreditreport.com](http://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](http://www.annualcreditreport.com)) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

---

### For residents of Iowa:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

---

### For residents of Oregon:

State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission.

---

### For residents of Maryland, Illinois, and North Carolina:

You can obtain information from the Maryland and North Carolina Offices of the Attorneys General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

<b>Maryland Office of the Attorney General</b> Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us	<b>North Carolina Office of the Attorney General</b> Consumer Protection Division 9001 Mail Service Center Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.gov	<b>Federal Trade Commission Consumer Response Center</b> 600 Pennsylvania Avenue, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/bcp/edu/microsites/idtheft
--	---	---

---

### For residents of Massachusetts:

It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

---

### For residents of all states:

**Fraud Alerts:** You can place fraud alerts with the three credit bureaus at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three credit bureaus is below.

**Monitoring:** You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

**Security Freeze:** You also have the right 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 need to send a request to each consumer reporting agency by certified mail, overnight mail, or regular stamped mail. 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 consumer reporting agency may charge a fee of up to \$5.00 to place a freeze or lift or remove a freeze, but is free if you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency. You may obtain a security freeze by contacting any one or more of the following national consumer reporting agencies:

<b>Equifax Security Freeze</b> P.O. Box 105788 Atlanta, GA 30348 www.equifax.com	<b>Experian Security Freeze</b> P.O. Box 9554 Allen, TX 75013 www.experian.com/freeze	<b>TransUnion (FVAD)</b> P.O. Box 2000 Chester, PA 19022 www.transunion.com
---	--	--

More information can also be obtained by contacting the Federal Trade Commission listed above.



## TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services<sup>1</sup> 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.

### **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.

<sup>1</sup> 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.