October 16, 2017

Gordon MacDonald
Attorney General
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301

Mr. MacDonald:

On behalf of Spark Pay Online Store ("SPOS"), a website hosting vendor and a now-former subsidiary of Capital One, N.A., I am writing to provide you with an update regarding an event that we alerted your Office to on July 6, 2017. That letter is attached for your convenience. As described in detail in the attached letter, the event involved malicious code on certain merchant websites that we host. The malicious code was designed to allow an unauthorized third party to obtain payment information when transactions were submitted on relevant merchant websites.

We have recently determined that the event occurred between March 10, 2017 and June 7, 2017. As a result, we have determined that the event may have involved certain websites hosted by SPOS for an additional 64 of our e-commerce merchant customers and payment information relating to an additional 144 New Hampshire residents.

On October 16, 2017, we will begin notifying each of the additional e-commerce merchants regarding this event, including providing them with information about their customers regarding whom information was involved in the event. In addition, out of an abundance of caution and in order to ensure consumers have the information they need, SPOS will be notifying 144 New Hampshire residents of this event by the week of October 23, 2017. We will provide these individuals with an offer for two years of complimentary credit monitoring. Attached is a sample of the letter that we are providing to New Hampshire residents.

Please do not hesitate to contact me at (301) 718-6800 if you have any questions.

Sincerely,

Christopher Peak
Vice President
Chief Counsel, International and Small Business
Capital One

Attachment

Capital One, N.A.
265 Broadhollow Rd.
Melville, NY 11747

<Date>

<F15> <F13> <F14>
<ENDORSE>
<F1>
<F2><F3> <F4>
<F6> <F7><F8>
<F5>
<F9>, <F10> <F11>-<F12>

NOTICE OF DATA BREACH

Dear customer of <P41 – URL>,

We wanted to let you know about a security event involving <P41 – URL> that included your payment information. Spark Pay® Online Store hosts this website and we want to provide you the details of this event and our offer of free credit monitoring.

WHAT HAPPENED. We discovered malicious code on the server that hosts <P41 – URL>. The code was designed to allow fraudsters to obtain customer payment information. We immediately began investigating the issue, analyzed the server, removed the malicious code and performed security testing.

WHAT INFORMATION WAS INVOLVED. Based on our investigation, we believe the fraudster may have accessed your name, address, phone number, email address, payment card number, expiration date, and CVV for any transactions you made on <P41 – URL> between <P1 – month day> and June 7, 2017.

WHAT WE ARE DOING. We are working with law enforcement and have notified Visa®, MasterCard®, Discover®, and American Express® who alerted the card issuing banks so that they can take appropriate steps to protect their cardholders in accordance with their fraud policies.

For your protection, we are providing two years of free credit monitoring and identity protection with TransUnion's credit monitoring service. You may sign up for this service at the website noted below by November 30, 2017. Please read the tips below on how to get started.

WHAT YOU CAN DO. We encourage you to monitor your payment card accounts, and if you notice any activity that you don't recognize, you should call the number on your card or statement as soon as possible. Per payment card rules, cardholders are not responsible for unauthorized charges reported in a timely manner.

We've also enclosed a list of tips for protecting yourself against potential misuse of your personal information.

FOR MORE INFORMATION. Please know that we regret any inconvenience or concern this incident may cause you. If you have any questions or concerns, please don't hesitate to call us at 1-844-383-0443, Monday-Friday, 8 a.m.-10 p.m. ET, and Saturday, 8 a.m.-7 p.m. ET.

Sincerely,

Celia Edwards Karam

Celia Edwards Karam
Managing Vice President
Spark Pay Online Store, a division of Capital One, N.A.

TIPS FOR SAFEGUARDING YOUR PERSONAL INFORMATION

1. We've arranged for you to enroll, for free, in an online three-bureau credit monitoring service (My TransUnion Monitoring) for two years. To enroll, go to www.transunionmonitoring.com and enter this unique 12-letter Activation Code: **<P56 - online code>.** Follow the simple three steps to receive your credit monitoring service online within minutes.
    - If you do not have access to the Internet, you may enroll in a similar offline paper-based three-bureau credit monitoring service. Call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422** and when prompted, enter the following 6-digit telephone pass code: **696627**.

    - **You can sign up for the online or offline credit monitoring service anytime between now and November 30, 2017.** Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and a valid Social Security number.

    - Once you're enrolled, you'll receive the following benefits at no cost to you:

        1. Two years of unlimited access to your TransUnion credit report and credit score.
        2. Daily monitoring of your TransUnion, Experian and Equifax credit reports.
        3. Alerts of potential fraud indicators across all three of your credit reports. Alerts include new inquiries, new accounts, new public records, late payments, change of address and more.
        4. Up to $1 million in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

2. Monitor your card account(s) carefully for incidents of fraud and identity theft over the next 12 to 24 months. If you discover any suspicious or unusual activity on your account(s) or suspect identity theft or fraud, report it immediately to your card issuing bank.

3. Monitor free credit reports. You can request and review credit reports from each nationwide credit reporting company noted below.

    - Once you receive your reports, review them for suspicious activity, such as inquiries from companies you did not contact, accounts you did not open, and debts that you did not authorize.

    - Notify the credit reporting company if any information is incorrect.

    To obtain a free copy of your credit report each year from the nationwide credit reporting companies, simply visit https://www.annualcreditreport.com/index.action, call **1-877-322-8228**, or complete the Annual Credit Report Request Form, which can be found at http://www.ftc.gov/bcp/edu/resources/forms/requestformfinal.pdf, and mail it to:

    Annual Credit Report Request Service
    P.O. Box 105281
    Atlanta, GA 30348-5281

    Additionally, you can call the toll-free fraud number of any one of the three nationwide credit reporting companies and place an initial fraud alert on your credit report. An initial fraud alert stays on your credit report for 90 days and acts as an alert to potential lenders to verify your identity.

Equifax
Consumer Fraud Division
P.O. Box 740256

Atlanta, GA 30374
1-800-525-6285
https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp

Experian
P.O. Box 9554
Allen, TX 75013
1-888-EXPERIAN (397-3742)
https://www.experian.com/fraud/center.html

TransUnion
Fraud Victim Assistance Division
P.O. Box 2000
Chester, PA 19022-2000
1-800-680-7289
http://www.transunion.com/fraud-victim-resource/place-fraud-alert

In addition, you can contact the nationwide credit reporting companies to place a security freeze to restrict access to your credit report. You will need to supply your name, address, date of birth, Social Security number and other personal information. The fee to place a credit freeze varies based on where you live. After receiving your request, each credit reporting company will send you a confirmation letter containing a unique PIN or password that you will need in order to lift or remove the freeze. You should keep the PIN or password in a safe place.

4. If you would like more information about precautions against identity theft, fraud alerts, security freezes or to report incidents of identity theft, you may contact the FTC or law enforcement. You may contact the FTC by visiting www.ftc.gov/idtheft, calling their hot line at **1-877-ID-THEFT (438-4338)** or writing them at:

   Federal Trade Commission Consumer Response Center
   600 Pennsylvania Avenue, N.W.
   Washington, DC 20580

IF YOU ARE AN IOWA RESIDENT: You may contact local law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. You can contact the Iowa Attorney General at:

Office of the Attorney General
1305 E. Walnut Street
Des Moines, IA 50319
(515) 281-5164
http://www.iowaattorneygeneral.gov/

IF YOU ARE A MARYLAND RESIDENT: You may obtain information about avoiding identity theft from the FTC or the Maryland Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
http://www.ftc.gov/idtheft/

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
www.oag.state.md.us

IF YOU ARE A NORTH CAROLINA RESIDENT: You may obtain information about preventing identity theft from the FTC or the North Carolina Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580

North Carolina Department of Justice
Attorney General Roy Cooper
9001 Mail Service Center
Raleigh, NC 27699-9001

(877) IDTHEFT (438-4338)
www.consumer.gov/idtheft

(877) 566-7226
http://www.ncdoj.com

IF YOU ARE A RHODE ISLAND RESIDENT: Please contact state or local law enforcement to determine whether you can file or obtain a police report in regard to this incident. In addition, you can contact the Rhode Island Attorney General at:

Office of the Attorney General
150 South Main Street
Providence, Rhode Island 02903
(401) 274-4400
http://www.riag.ri.gov/

FM57850_001_001

July 6, 2017

Gordon MacDonald
Attorney General
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301

Mr. MacDonald:

On behalf of Spark Pay Online Store ("SPOS"), a website hosting vendor and a division of Capital One, N.A., I am writing to inform you about a recent event involving certain websites hosted by SPOS for 175 of our e-commerce merchant customers. As discussed below, the event involved an unauthorized third party potentially obtaining payment information relating to 120 New Hampshire residents. Some of these merchants may have already alerted you to this event. Nonetheless, we are sending you this letter to ensure that you are aware of the event.

On June 6, 2017, we discovered malicious code on certain merchant websites that we host. The malicious code was designed to allow an unauthorized third party to obtain payment information when transactions were submitted on the relevant merchant websites. Through our investigation, we have determined that the unauthorized third party may have obtained the name, address, phone number, email address, payment card number, expiration date, and CVV for certain individuals who made purchases on these websites between April 10, 2017 and June 7, 2017.

Upon discovering the malicious code, we took the relevant merchant websites offline and immediately began conducting an investigation. Before bringing the websites back online, we analyzed the sites, removed the malicious code and performed security testing. We also alerted the Federal Bureau of Investigation. In addition, we alerted the payment card networks so that they could notify their card issuing banks to take steps to protect their cardholders in accordance with their fraud policies.

On June 15, 2017, we also notified each of our relevant e-commerce merchant customers regarding this event, including providing them with information about their customers regarding whom information was involved in this event. In addition, out of an abundance of caution and in order to ensure consumers have the information they need, SPOS will be notifying 120 New Hampshire residents of this event by the week of July 17, 2017. We will provide these individuals with an offer for two years of complimentary credit monitoring. Attached is a sample of the letter that we are providing to New Hampshire residents.

Please do not hesitate to contact me at (301) 718-6800 if you have any questions.

Sincerely,

Christopher Peak
Vice President
Chief Counsel, International and Small Business
Capital One

Attachment

Capital One, N.A.
265 Broadhollow Rd.
Melville, NY 11747

<Date>

<F15> <F13> <F14>
<ENDORSE>
<F1>
<F2><F3> <F4>
<F6> <F7><F8>
<F5>
<F9>, <F10> <F11>-<F12>k,

NOTICE OF DATA BREACH

Dear [merchant website] customer,

We wanted to let you know about a security event involving [merchant website] that included your payment information. Spark Pay® Online Store hosts this website and we want to provide you the details of this event and our offer of free credit monitoring.

WHAT HAPPENED. We discovered malicious code on [merchant website]. The code was designed to allow fraudsters to obtain customer payment information. We immediately began investigating the issue, analyzed [merchant website], removed the malicious code and performed security testing.

WHAT INFORMATION WAS INVOLVED. Based on our investigation, we believe the fraudster may have accessed your name, address, phone number, email address, payment card number, expiration date, and CVV for any transactions you made on [merchant website] between [variable dates between April 10, 2017 and June 7, 2017].

WHAT WE ARE DOING. We are working with law enforcement and have notified Visa®, MasterCard®, Discover®, and American Express® who alerted the card issuing banks so that they can take appropriate steps to protect their cardholders in accordance with their fraud policies.

For your protection, we are providing two years of free credit monitoring and identity protection with TransUnion's credit monitoring service. You may sign up for this service at the website noted below by September 30, 2017. Please read the tips below on how to get started.

WHAT YOU CAN DO. We encourage you to monitor your payment card accounts, and if you notice any activity that you don't recognize, you should call the number on your card or statement as soon as possible. Per payment card rules, cardholders are not responsible for unauthorized charges reported in a timely manner.

We've also enclosed a list of tips for protecting yourself against potential misuse of your personal information.

FOR MORE INFORMATION. Please know that we regret any inconvenience or concern this incident may cause you. If you have any questions or concerns, please don't hesitate to call us at 1-844-383-0443, Monday-Friday, 8 a.m.-10 p.m. ET, and Saturday, 8 a.m.-7 p.m. ET.

Sincerely,

Celia Edwards Karam
Managing Vice President
Spark Pay Online Store, a division of Capital One, N.A.

TIPS FOR SAFEGUARDING YOUR PERSONAL INFORMATION

1. We've arranged for you to enroll, for free, in an online three-bureau credit monitoring service (My TransUnion Monitoring) for two years. To enroll, go to www.transunionmonitoring.com and enter this unique 12-letter Activation Code: **<online code>.** Follow the simple three steps to receive your credit monitoring service online within minutes.
    - If you do not have access to the Internet, you may enroll in a similar offline paper-based three-bureau credit monitoring service. Call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422** and when prompted, enter the following 6-digit telephone pass code: **696627**.

    - **You can sign up for the online or offline credit monitoring service anytime between now and September 30, 2017.** Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and a valid Social Security number.

    - Once you're enrolled, you'll receive the following benefits at no cost to you:

        1. Two years of unlimited access to your TransUnion credit report and credit score.
        2. Daily monitoring of your TransUnion, Experian and Equifax credit reports.
        3. Alerts of potential fraud indicators across all three of your credit reports. Alerts include new inquiries, new accounts, new public records, late payments, change of address and more.
        4. Up to $1 million in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

2. Monitor your card account(s) carefully for incidents of fraud and identity theft over the next 12 to 24 months. If you discover any suspicious or unusual activity on your account(s) or suspect identity theft or fraud, report it immediately to your card issuing bank.

3. Monitor free credit reports. You can request and review credit reports from each nationwide credit reporting company noted below.

    - Once you receive your reports, review them for suspicious activity, such as inquiries from companies you did not contact, accounts you did not open, and debts that you did not authorize.

    - Notify the credit reporting company if any information is incorrect.

    To obtain a free copy of your credit report each year from the nationwide credit reporting companies, simply visit https://www.annualcreditreport.com/index.action, call **1-877-322-8228**, or complete the Annual Credit Report Request Form, which can be found at http://www.ftc.gov/bcp/edu/resources/forms/requestformfinal.pdf, and mail it to:

    Annual Credit Report Request Service
    P.O. Box 105281
    Atlanta, GA 30348-5281

    Additionally, you can call the toll-free fraud number of any one of the three nationwide credit reporting companies and place an initial fraud alert on your credit report. An initial fraud alert stays on your credit report for 90 days and acts as an alert to potential lenders to verify your identity.

Equifax
Consumer Fraud Division
P.O. Box 740256
Atlanta, GA 30374
1-800-525-6285
https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp

Experian
P.O. Box 9554
Allen, TX 75013
1-888-EXPERIAN (397-3742)
https://www.experian.com/fraud/center.html

TransUnion
Fraud Victim Assistance Division
P.O. Box 2000
Chester, PA 19022-2000
1-800-680-7289
http://www.transunion.com/fraud-victim-resource/place-fraud-alert

In addition, you can contact the nationwide credit reporting companies to place a security freeze to restrict access to your credit report. You will need to supply your name, address, date of birth, Social Security number and other personal information. The fee to place a credit freeze varies based on where you live. After receiving your request, each credit reporting company will send you a confirmation letter containing a unique PIN or password that you will need in order to lift or remove the freeze. You should keep the PIN or password in a safe place.

4. If you would like more information about precautions against identity theft, fraud alerts, security freezes or to report incidents of identity theft, you may contact the FTC or law enforcement. You may contact the FTC by visiting www.ftc.gov/idtheft, calling their hot line at **1-877-ID-THEFT (438-4338)** or writing them at:

   Federal Trade Commission Consumer Response Center
   600 Pennsylvania Avenue, N.W.
   Washington, DC 20580

IF YOU ARE AN IOWA RESIDENT: You may contact local law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. You can contact the Iowa Attorney General at:

Office of the Attorney General
1305 E. Walnut Street
Des Moines, IA 50319
(515) 281-5164
http://www.iowaattorneygeneral.gov/

IF YOU ARE A MARYLAND RESIDENT: You may obtain information about avoiding identity theft from the FTC or the Maryland Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
http://www.ftc.gov/idtheft/

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
www.oag.state.md.us

IF YOU ARE A NORTH CAROLINA RESIDENT: You may obtain information about preventing identity theft from the FTC or the North Carolina Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
www.consumer.gov/idtheft

North Carolina Department of Justice
Attorney General Roy Cooper
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
http://www.ncdoj.com

IF YOU ARE A RHODE ISLAND RESIDENT: Please contact state or local law enforcement to determine whether you can file or obtain a police report in regard to this incident. In addition, you can contact the Rhode Island Attorney General at:

Office of the Attorney General
150 South Main Street
Providence, Rhode Island 02903
(401) 274-4400
http://www.riag.ri.gov/

FM57850_001_001