



Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<mail id>>
<<Name>>
<<Address1>>
<<Address2>>
<<City>><<State>><<Zip>>

<<Date>>

Dear <<Name>>,

MMF POS, a division of Block and Company, Inc., recently discovered that we were the target of a criminal cyber attack that may have impacted certain of your personal information. We value and respect your privacy, which is why we are writing to advise you of the steps that Block and Company has undertaken since discovering the incident and to provide you with information on what you can do to better protect yourself, should you feel it is appropriate to do so.

On March 21, 2016, we discovered that malicious code had been placed on our web server on or about February 9, 2016. Although our investigation is ongoing, we believe that the malware may have targeted your personal information, including your first and last name, billing or mailing address, email address, and credit card information (card holder name, credit card account number, expiration month and year, and card security code).

We promptly launched an internal investigation, and we engaged a premier cybersecurity firm to assist in our containment and remediation efforts as well as to conduct a forensic investigation. We also notified law enforcement, including the Federal Bureau of Investigation, and we continue to work closely with their criminal investigation.

In addition to conducting an extensive internal investigation and working with law enforcement, we are implementing further security protections, in addition to our existing measures, to help prevent this type of incident from occurring in the future, including the installation of a Website Application Firewall/Intrusion Prevention System (WAF/IPS) that proactively mitigates attacks against our website. The website is also scanned several times a day using technology that is capable of identifying any Indicator of Compromise (IoC) and is able to quickly identify and alert our staff in the event of any security incident.

We have also established a confidential inquiry line to assist you with any questions regarding this incident. This confidential inquiry line is available between 9 a.m. and 9 p.m., Eastern time, Monday through Friday, at 1-844-778-5954.

We value the trust you place in Block and Company to protect the privacy and security of your personal information, and we regret any inconvenience or concern that this incident might cause you.

Sincerely,

John Cruickshank
Vice President of Finance and Chief Financial Officer
Block and Company, Inc.

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your credit card account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes, and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at: www.annualcreditreport.com/cra/requestformfinal.pdf.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries, including obtaining information about fraud alerts and placing a security freeze on your credit files, is as follows:

Equifax
1-800-349-9960
www.equifax.com
P.O. Box 105788
Atlanta, GA 30348

Experian
1-888-397-3742
www.experian.com
P.O. Box 9554
Allen, TX 75013

TransUnion
1-888-909-8872
www.transunion.com
P.O. Box 2000
Chester, PA 19022

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that creditors contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Credit and Security Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze on your credit file, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may cause a delay should you attempt to obtain credit. In addition, you may incur fees for placing, lifting, and/or removing a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state—generally \$5 to \$20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013

TransUnion Security Freeze
Fraud Victim Assistance
Department
P.O. Box 6790
Fullerton, CA 92834

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

Maryland Residents: Maryland residents can contact the Office of the Attorney General at:
Office of the Attorney General
220 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
www.oag.state.md.us

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
www.ncdoj.com



Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<mail id>>
<<Name>>
<<Address1>>
<<Address2>>
<<City>><<State>><<Zip>>

<<Date>>

Dear <<Name>>,

MMF Industries, a division of Block and Company, Inc., recently discovered that we were the target of a criminal cyber attack that may have impacted certain of your personal information. We value and respect your privacy, which is why we are writing to advise you of the steps that Block and Company has undertaken since discovering the incident and to provide you with information on what you can do to better protect yourself, should you feel it is appropriate to do so.

On March 21, 2016, we discovered that malicious code had been placed on our web server on or about February 9, 2016. Although our investigation is ongoing, we believe that the malware may have targeted your personal information, including your first and last name, billing or mailing address, email address, and credit card information (card holder name, credit card account number, expiration month and year, and card security code).

We promptly launched an internal investigation, and we engaged a premier cybersecurity firm to assist in our containment and remediation efforts as well as to conduct a forensic investigation. We also notified law enforcement, including the Federal Bureau of Investigation, and we continue to work closely with their criminal investigation.

In addition to conducting an extensive internal investigation and working with law enforcement, we are implementing further security protections, in addition to our existing measures, to help prevent this type of incident from occurring in the future, including the installation of a Website Application Firewall/Intrusion Prevention System (WAF/IPS) that proactively mitigates attacks against our website. The website is also scanned several times a day using technology that is capable of identifying any Indicator of Compromise (IoC) and is able to quickly identify and alert our staff in the event of any security incident.

We have also established a confidential inquiry line to assist you with any questions regarding this incident. This confidential inquiry line is available between 9 a.m. and 9 p.m., Eastern time, Monday through Friday, at 1-844-778-5954.

We value the trust you place in Block and Company to protect the privacy and security of your personal information, and we regret any inconvenience or concern that this incident might cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "John Cruickshank", with a stylized flourish at the end.

John Cruickshank
Vice President of Finance and Chief Financial Officer
Block and Company, Inc.

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your credit card account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes, and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at: www.annualcreditreport.com/cra/requestformfinal.pdf.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries, including obtaining information about fraud alerts and placing a security freeze on your credit files, is as follows:

Equifax
1-800-349-9960
www.equifax.com
P.O. Box 105788
Atlanta, GA 30348

Experian
1-888-397-3742
www.experian.com
P.O. Box 9554
Allen, TX 75013

TransUnion
1-888-909-8872
www.transunion.com
P.O. Box 2000
Chester, PA 19022

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that creditors contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Credit and Security Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze on your credit file, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may cause a delay should you attempt to obtain credit. In addition, you may incur fees for placing, lifting, and/or removing a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state—generally \$5 to \$20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013

TransUnion Security Freeze
Fraud Victim Assistance
Department
P.O. Box 6790
Fullerton, CA 92834

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

Maryland Residents: Maryland residents can contact the Office of the Attorney General at:

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

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
www.ncdoj.com



Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<mail id>>
<<Name>>
<<Address1>>
<<Address2>>
<<City>><<State>><<Zip>>

<<Date>>

Dear <<Name>>,

Block and Company, Inc. recently discovered that we were the target of a criminal cyber attack that may have impacted certain of your personal information. We value and respect your privacy, which is why we are writing to advise you of the steps that Block and Company has undertaken since discovering the incident and to provide you with information on what you can do to better protect yourself, should you feel it is appropriate to do so.

On March 1, 2016, we discovered that malicious code had been placed on our web server on or about February 9, 2016. Although our investigation is ongoing, we believe that the malware may have targeted your personal information, including your first and last name, billing or mailing address, email address, and credit card information (card holder name, credit card account number, expiration month and year, and card security code).

We promptly launched an internal investigation, and we engaged a premier cybersecurity firm to assist in our containment and remediation efforts as well as to conduct a forensic investigation. We also notified law enforcement, including the Federal Bureau of Investigation, and we continue to work closely with their criminal investigation.

In addition to conducting an extensive internal investigation and working with law enforcement, we are implementing further security protections, in addition to our existing measures, to help prevent this type of incident from occurring in the future, including the installation of a Website Application Firewall/Intrusion Prevention System (WAF/IPS) that proactively mitigates attacks against our website. The website is also scanned several times a day using technology that is capable of identifying any Indicator of Compromise (IoC) and is able to quickly identify and alert our staff in the event of any security incident.

We have also established a confidential inquiry line to assist you with any questions regarding this incident. This confidential inquiry line is available between 9 a.m. and 9 p.m., Eastern time, Monday through Friday, at 1-844-778-5954.

We value the trust you place in Block and Company to protect the privacy and security of your personal information, and we regret any inconvenience or concern that this incident might cause you.

Sincerely,

John Cruickshank
Vice President of Finance and Chief Financial Officer
Block and Company, Inc.

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your credit card account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes, and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at: www.annualcreditreport.com/cra/requestformfinal.pdf.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries, including obtaining information about fraud alerts and placing a security freeze on your credit files, is as follows:

Equifax
1-800-349-9960
www.equifax.com
P.O. Box 105788
Atlanta, GA 30348

Experian
1-888-397-3742
www.experian.com
P.O. Box 9554
Allen, TX 75013

TransUnion
1-888-909-8872
www.transunion.com
P.O. Box 2000
Chester, PA 19022

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that creditors contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Credit and Security Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze on your credit file, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may cause a delay should you attempt to obtain credit. In addition, you may incur fees for placing, lifting, and/or removing a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state—generally \$5 to \$20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013

TransUnion Security Freeze
Fraud Victim Assistance
Department
P.O. Box 6790
Fullerton, CA 92834

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

Iowa Residents: 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
www.iowaattorneygeneral.gov

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
www.ncdoj.com