

September 22, 2023

**Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202**

Re: Block, Inc. – Notice of Account Takeover Incident

Dear Sir or Madam:

I am writing to provide notification of an account takeover incident at Block, Inc., formerly known as “Square, Inc.” (“Block”) that may have affected the security of personal information of some Maryland residents.

Block recently identified a pattern of account takeovers where unauthorized actors were using recycled phone numbers that were registered to Cash App accounts to authenticate into those Cash App accounts. These bad actors exploited a vulnerability that allowed them to login to the associated Cash App accounts by providing a code sent to the recycled phone number without providing any additional information typically required to authenticate new devices. On September 19, 2023, Block determined that these actors accessed, and in some cases, downloaded different types of personal information which may have included: the name of the resident, Cash App Card number, expiration date, and CVV for 184 Maryland residents between January 12, 2023 – June 19, 2023. Additionally, the Social Security numbers for 24 residents were in the accounts at the time of the activity and may have been accessed.

Block has stopped the activity by patching the vulnerability through a software update of the affected systems and retained forensic experts to investigate the scope and impact of the incident. They are taking steps to reimburse customers and have also notified law enforcement.

Block is in the process of providing the accountholders whose personal information was affected with written notification of this incident. For individuals whose Social Security number may have been affected, they are also being provided two years of free credit monitoring services. Block is also advising the affected residents about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At Block, protecting the privacy of personal information is a top priority. Block is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it, and continually evaluates and modifies its practices and internal controls to enhance the security and privacy of personal information.

Should you have any questions concerning this notification, please contact me at 206-839-4300 or jsantiesteban@orrick.com. Thank you.

Page 2

Very truly yours,
Joe Santiesteban

Encl.

Via First Class Mail

[Name]
[Address]

Re: Notice of Security Incident

Dear [Recipient Name],

We are writing to follow up regarding a suspicious login to your Cash App account and our efforts to strengthen the security of your account. This notice provides information about what happened and what we are doing about it.

What Happened?

We recently identified a suspicious login to your Cash App account. At the time, we sent you an email and/or text message regarding a sign-in from a new device. We initiated an investigation and retained cybersecurity experts to assist us with the investigation to determine what happened and what data was affected. We have now determined that an unauthorized user logged into your Cash App account using a phone number that was linked to your account and had been recycled by your carrier. This can happen, for example, when your carrier decides a number is no longer in use by you, and the carrier gives that number to a new person.

[We have canceled your Cash App Card for your protection, and you can order a new Cash App Card in the app. You still have access to your existing Cash App account.]

What Information Was Involved?

[Your name, [Cash App account number and routing number], Cash App Card number, expiration date, and CVV appear to have been [downloaded/accessed] [on or about [date]]. **Your external personal bank account or card information that you connected to Cash App were NOT affected. Your Social Security number and driver's license information were also NOT affected. Given that we have canceled the card, there is no ongoing risk that this card may be used fraudulently in the future.]**

[Your name, [Cash App account number and routing number], Cash App Card number, expiration date, and CVV appear to have been [downloaded/accessed] [on or about [date]]. While your Social Security number [and brokerage account number] are also contained in your Cash App account, we have no evidence this information was accessed or downloaded. **Your external personal bank account or card information that you connected to Cash App were NOT affected. Given that we have canceled the card, there is no ongoing risk that this card may be used fraudulently in the future.]**

[Your name, [Cash App account number and routing number], Cash App Card number, expiration date, and CVV appear to have been [downloaded/accessed] [on or about [date]]. While your brokerage account number is also contained in your Cash App account, we have no evidence this information was accessed or downloaded. **Your external personal bank account or card information that you connected to Cash App were NOT affected. Your Social Security number and driver's license information were NOT affected. Given that we have canceled the card, there is no ongoing risk that this card may be used fraudulently in the future.]**

What We Are Doing:

[We are offering you two years of credit monitoring services through Cyberscout through Identity Force, a TransUnion company, at no cost. Registration instructions are included in this letter.]

We have also notified law enforcement and remain committed to continuously improving our security policies and procedures.

What You Can Do:

[In addition to signing up for credit monitoring,] Cash App's security monitoring is here to help keep your account safe, and here are some additional steps you can take:

- Regularly review and monitor your account statements and credit history for any signs of unauthorized transactions or activity.
- Keep your contact information up to date and review devices that are signed in to your Cash App account in the Settings section of the app.
- Protect your Cash App account by turning on two-factor authentication for sign in and enabling the Security Lock setting so that every Cash App payment and unmasking your Cash App Card number requires your passcode, Touch ID or Face ID.

For more information:

If you have questions, please contact customer support via the app or by phone at 1 (800) 969-1940, Monday through Friday, 9:00am to 7:00pm EST.

Sincerely,

Your Cash App Team

Securities offered by Cash App Investing LLC, a subsidiary of Block, Inc. and member FINRA/SIPC.

Appendix

[Instructions for Credit Monitoring Services]

In response to the incident, we are providing you with access to credit monitoring services at no charge. These services provide you with alerts for twenty-four (24) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to <https://secure.identityforce.com/benefit/block> and follow the instructions provided. When prompted please provide the following unique code to receive services: <CODE HERE>

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.]

Below are additional helpful tips you may want to consider to protect your personal information.

Review Your Credit Reports and Account Statements; Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your credit reports and account statements closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or other company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities. 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 law enforcement, the Federal Trade Commission ("FTC") and/or the Attorney General's office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft, and you can contact the FTC at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
<http://www.identitytheft.gov/>
1-877-IDTHEFT (438-4338)

Copy of Credit Report

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <https://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print this form at <https://www.annualcreditreport.com/manualRequestForm.action>. Credit reporting agency contact details are provided below.

Equifax:
equifax.com
equifax.com/personal/credit-report-services
P.O. Box 740241
Atlanta, GA 30374
800-685-1111

Experian:
experian.com
experian.com/help
P.O. Box 2002
Allen, TX 75013
888-397-3742

TransUnion:
transunion.com
transunion.com/credit-help
P.O. Box 1000
Chester, PA 19016
888-909-8872

When you receive your credit reports, review them carefully. Look for accounts or credit inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is inaccurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Fraud Alert

You may want to consider placing a fraud alert on your credit file. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. If you have already been a victim of identity theft, you may have an extended alert placed on your report if you provide the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above.

Security Freeze

You have the right to place a security freeze on your credit file free of charge. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may delay your ability to obtain credit. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name; social security number; date of birth; current and previous addresses; a copy of your state-issued identification card; and a recent utility bill, bank statement, or telephone bill.

Federal Fair Credit Reporting Act Rights

The Fair Credit Reporting Act ("FCRA") is federal legislation that regulates how consumer reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of consumer reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. Identity theft victims and active-duty military personnel have additional rights.

For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Avenue N.W., Washington, D.C. 20580.

Additional Information

If you are the victim of fraud or identity theft, you also have the right to file a police report.

You may consider starting a file with copies of your credit reports, any police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

For Colorado and Illinois residents: You may obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes.

For District of Columbia residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 110 South, Washington D.C. 20001, <https://www.oag.dc.gov/>, 1-202-727-3400.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the state Attorney General.

For Maryland residents: You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, <http://www.marylandattorneygeneral.gov>, 1-888-743-0023. The Office of the Maryland Attorney General may be able to provide you with information about the steps you can take to avoid identity theft.

For Massachusetts residents: You have the right to obtain a police report regarding this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For New York residents: For more information on identity theft, you can contact the following: New York Department of State Division of Consumer Protection at <http://www.dos.ny.gov/consumerprotection> or (800) 697-1220 or NYS Attorney General at <http://www.ag.ny.gov/home.html> or (800) 771-7755.

For New Mexico Residents: You have rights pursuant to the FCRA, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the FCRA, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the FCRA not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the FCRA. We encourage you to review your rights pursuant to the FCRA by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001, <http://www.ncdoj.gov>, 1-877-566-7226. You are also advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General. For more information on security locks, you can visit the Oregon Department of Consumer and Business Services website at <https://dfr.oregon.gov/financial/protect/Pages/stolen-identity.aspx> and click “Place a credit freeze.”

For Rhode Island residents: The Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this event.

For Arizona, California, Iowa, Montana, New York, North Carolina, Oregon, Washington, Washington, D.C., and West Virginia 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 bureaus directly to obtain such additional report(s).