Annmarie Nowak
VP, Operational Risk, Data and Privacy

777 Long Ridge Road
Stamford, CT 06902

203-585-2026
annmarie.nowak@syf.com

Via email to: DOJ-CPB@DOJ.NH.GOV

Consumer Protection Bureau
Attorney General Gordon MacDonald
New Hampshire Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

November 27, 2018

Dear Attorney General MacDonald:

Pursuant to NH Rev Stat s.359-C:20, we are writing to notify you of a security breach involving 28 residents of New Hampshire. We understand that you may also be notified of this incident by Stein Mart, Inc.

We have been advised by Stein Mart, Inc. that during certain periods between December 28, 2017 and July 9, 2018, the personal information of individuals holding a credit card issued by Synchrony Bank may have been obtained by unauthorized persons when shopping online at www.steinmart.com. We understand that a web site application provided by a third-party vendor of Stein Mart, Inc., used on www.steinmart.com, contained unauthorized code. When the impacted cardholders used their credit card to complete a purchase on this web site, they may have been targeted by this unauthorized code allowing access to some of their personal information including name, address, email address, credit account number, security code and expiration date relating to the credit card. We have been advised by Stein Mart, Inc. that the unauthorized code (and the third-party login feature) was removed from the website.

Upon learning about this incident, Synchrony Bank promptly began working with Stein Mart, Inc. to obtain data that would allow us to determine what had occurred. In addition, when we discovered potential fraudulent activity, we began closely monitoring the potentially impacted accounts for unauthorized activity and proactively implemented mitigation actions. It should be noted that this incident did not result from any actions by Synchrony Bank or any compromise of any Synchrony Bank systems or processes.

The impacted residents of New Hampshire will be notified by mail in the next few days. A copy of the notification is enclosed. The cardholders impacted will be offered one year of credit monitoring at no cost to the cardholder.

If you have any questions, you can contact me at (203) 585-2026.

Sincerely,

Annmarie Nowak

SYNCHRONY BANK
PO BOX 965003
Orlando, FL 32896-5003

[CARDHOLDER NAME]
[STREET ADDRESS]
[CITY, STATE AND POSTAL CODE]

Re: Possible Disclosure of Personal Information

CURRENT DATE

Dear [CARDHOLDER NAME]:

We recently learned that information associated with your [card name] may have been obtained by unauthorized users at some point between December 28, 2017 and July 9, 2018. Upon learning about this incident, Synchrony Bank promptly began working with Stein Mart, Inc. to gather data that would allow us to clearly determine what had occurred.

Stein Mart, Inc. has advised us that a web site application provided by a third-party vendor of Stein Mart, Inc., and used on www.steinmart.com, contained unauthorized code. The information entered by you when you used your credit card to complete your purchase on www.steinmart.com may have been targeted by this unauthorized code. Unfortunately, this may have allowed access to some of your personal information including your name, address, email address, credit account number, security code and expiration date for your [card name]. We understand the unauthorized code was removed and the third-party vendor's login feature was also removed from the website. It is important to note that this incident did not result from any actions by Synchrony Bank or compromise of any of our systems or processes.

As a result of this incident, a new credit card may be issued to you with updated security credentials. In addition, we would like to offer you a one-year subscription to a credit report monitoring service at no cost to you. If you would like to receive the credit report monitoring service or have any questions, contact us at 1-866-834-3206 (Monday through Friday from 8 a.m. to 5 p.m. ET) within 90 days of the date on this letter.

To protect yourself further, you may also consider:

1. Placing a fraud alert on your credit files: The fraud alert is free and will require that potential creditors to verify your identity before issuing credit in your name, thereby reducing or hopefully eliminating the likelihood of an unauthorized account. The fraud alert is renewable every 90 days. A call to any one of the three credit reporting agencies listed below will place a fraud alert on your credit file with all three agencies. You will receive letters from the agencies confirming the fraud alert and informing you about how to get a free copy of your credit report. Here's how to contact them:

    - Equifax: 800-685-1111 or www.equifax.com/personal/credit-report-services
    - Experian: 888-397-3742 or www.experian.com/help
    - TransUnion: 888-909-8872 or www.transunion.com/credit-help

2. Obtaining and reviewing your credit bureau report: Examine it carefully, looking for accounts you did not open, inquiries from creditors you did not initiate or personal information that is not accurate and contact the credit reporting agency that provided the report with any questions. If you do find suspicious activity on your credit reports, you should also contact your local police or Sheriff's office to file a report of identity theft. Make sure to ask for a copy of the police report as you may need to provide copies to creditors to clear up your records. Even if you do not find any signs of fraud on your reports, it's always good idea to review your credit bureau reports periodically to make sure they are accurate.

3. Adding a "security freeze" on your credit file: A "security freeze" will prevent new credit accounts from being opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. You must separately place a security freeze on your credit file with each credit reporting agency identified above. Please note that using a security freeze may delay your ability to obtain credit.

For more information on identity theft, visit the Federal Trade Commission's web site at www.ftc.gov/idtheft.

[Maryland residents may review information provided by the Maryland Attorney General on how to avoid identity theft at http://www.oag.state.md.us/idtheft, or by sending an email to idtheft@oag.statemd.us, or calling 410-576-6491.]

[North Carolina residents may review information provided by the North Carolina Attorney General at http://www.ncdoj.gov, by calling 877-566-7226, or writing to 9001 Mail Service Center, Raleigh, NC 27699.]

[Rhode Island residents may review information provided by the Rhode Island Attorney General at http://www.riag.ri.gov by calling 401-274-4400, or writing to 150 South Main Street Providence, Rhode Island 02903.]

If you have any questions or need further assistance, our team is here to help.

Sincerely,

Synchrony Bank Fraud Management