



*Making Life Better*

**Main Office**  
312 Palmer Avenue  
Corinth, NY 12822  
Phone: 518-654-9028  
Toll-Free: 1-800-824-0700  
Fax: 518-654-7234

**Cohoes Office**  
98 Niver Street  
Cohoes, NY 12047  
Phone: 518-237-1121  
Fax: 518-237-1122

**Glens Falls Office**  
160 Broad Street  
Glens Falls, NY 12801  
Phone: 518-743-0561  
Fax: 518-745-0870

Loan Express: 1-800-211-8056 • Web Site: [www.HRcreditunion.org](http://www.HRcreditunion.org)

---

January 25, 2007

New York State Consumer Protection Board  
5 Empire State Plaza  
Albany, NY 12223

To Whom It May Concern:

This letter is to inform you that our credit union had debit and credit cards that were compromised in the TJX Companies, Inc. data breach. We have been notifying members as we receive notification from our card processor. After reviewing the depth of the information compromised and discussions with our insurance company we have determined we will be blocking and reissuing all the cards involved.

There were 2,071 active VISA debit and credit cards we have been notified were affected.

If you need any other information regarding this issue please do not hesitate to call me.

Sincerely yours,

A handwritten signature in cursive script that reads "Susan E. Commanda".

Susan E. Commanda, CEO  
Hudson River Community Credit Union

Enc

NYS CONSUMER  
PROTECTION BOARD

FEB 02 2007

RECEIVED



January 24, 2007

To Our Dear Valued Customer:

Since our customers have always been and will continue to be our highest priority, I regret to report to you that there has been an unauthorized intrusion into our computer systems that process and store information related to customer transactions for our T.J. Maxx, Marshalls, HomeGoods and A.J. Wright stores in the U.S. We have specifically identified a relatively small number of customer names and addresses with related driver's license numbers that were stolen from our computer systems, and we are writing to notify you that your information was among the data stolen. We deeply regret any difficulties this incident may cause you.

We are working closely with law enforcement in the investigation of this crime. We urge you to protect yourself by closely monitoring your account statements and taking steps against possible identity fraud. In particular, we recommend that you take the following precautions:

Contact Your Local Department of Motor Vehicles. Because your driver's license number has been accessed, we recommend that you immediately contact your local department of motor vehicles. Ask them to put a fraud alert on your license. This alert should notify the department of any attempts to tamper with your driver's license.

Place a One-Call, 90-Day Fraud Alert on Your Credit Report. Contact one of these credit bureaus to place a fraud alert on your credit file:

|            |              |                                                            |                                                                                |
|------------|--------------|------------------------------------------------------------|--------------------------------------------------------------------------------|
| Equifax    | 800-525-6285 | <a href="http://www.equifax.com">www.equifax.com</a>       | P.O. Box 740241<br>Atlanta, GA 30374-0241                                      |
| Experian   | 888-397-3742 | <a href="http://www.experian.com">www.experian.com</a>     | P.O. Box 9532<br>Allen, TX 75013                                               |
| TransUnion | 800-680-7289 | <a href="http://www.transunion.com">www.transunion.com</a> | Fraud Victim Assistance<br>Division, P.O. Box 6790<br>Fullerton, CA 92834-6790 |

You only need to call one of the three credit bureaus; the one you contact is required by law to contact the other two. This one-call fraud alert will remain in your credit file for at least 90 days. The fraud alert requires creditors to contact you before opening any new accounts or increasing credit limits on your existing accounts. When you place a fraud alert on your credit report, all three credit bureaus are required to send you a credit report free of charge.

Placing a fraud alert on your credit file helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone

applying for credit, the merchant gets a notice that there may be fraud on the account. This alerts the merchant to take steps to verify the identity of the applicant.

**Order Your Free Credit Report and Look for Unauthorized Activity.** You are entitled under U.S. law to one free credit report annually from each of the three national credit bureaus listed above. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com), call toll-free at 877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's website ([www.ftc.gov](http://www.ftc.gov)) and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. To obtain free annual credit reports, you must request them through this website, toll-free number or address. You should not contact the credit bureaus directly to get your free credit report.

When you receive your credit report, please review it carefully. Look for accounts you don't recognize. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Although some companies bill under names other than their store names, the credit bureau will be able to tell you when that is the case. And look in the "personal information" section for information (such as your home address or Social Security number) that is inaccurate. Such errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so that the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing.

If you have any trouble understanding your credit report, you should call the credit bureaus at the numbers given on their reports. Their staff will review your report with you. If the information cannot be explained, then you will need to call the creditors involved. You should also report information that cannot be explained to your local police or sheriff's office, because it may signal criminal activity.

If you believe your identity has been stolen, we recommend that you take the following steps:

**Follow the Federal Trade Commission's Guidelines.** These guidelines (available at [www.ftc.gov](http://www.ftc.gov)) are:

- (1) **Close the accounts** that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)) when you dispute new unauthorized accounts.
- (2) **File a Local Police Report.** Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.
- (3) **File your Concern with the FTC.** The FTC maintains a database of identity theft cases used by law enforcement agencies for their investigations. By filing a concern, you can help the FTC learn more about identity theft and the problems victims are having. The FTC's Identity Theft Hotline toll-free number is 877-IDTHEFT (877-438-4338) or you can visit their website at [www.ftc.gov](http://www.ftc.gov).


**Consider Placing an Extended Fraud Alert on Your Credit File.** If after reviewing your credit report you believe there is unexplained activity indicating possible identity theft, you may want to place an extended fraud alert on your credit report. In order to do this, you need to file a police report with your local police department, keep a copy for yourself, and provide a copy to one of the three major credit bureaus. This will entitle you to an extended fraud alert on your credit file for a 7-year period.

For your additional protection, please note that we will not call or email you requesting any credit card, PIN, or other personal information. If you do receive an email that appears to be from TJX or one of our stores, please use caution and do not provide personal information in response to any such calls or emails.

I hope this information is useful to you. For more details, please visit our website at [www.tjx.com](http://www.tjx.com). We have set up a special toll-free number for customers whose names, addresses and drivers' license numbers have been stolen. If you would like to speak with us, please call us at this special number: (888) 444-6299.

Again, I deeply regret any difficulties that this unauthorized intrusion may cause you and am hopeful that the information we are providing will be helpful.

Sincerely,



Ben Cammarata  
Chairman

**PLEASE SUBMIT THIS FORM TO ALL THREE (3) STATE AGENCIES as follows:**

**Fax** this form to the Consumer Protection Board (CPB):

**CPB:**

Security Breach Notification-

Fax: 518-474-2474

and also **Fax & Mail** this form to:

**NYS Office of Cyber Security and Critical Infrastructure Coordination (CSCIC):**

30 South Pearl St.

Floor P2

Albany, NY 12207

Fax: 518-474-9090

**Attorney General:**

Asst. Attorney General in Charge

Bureau of Consumer Frauds

120 Broadway - 3<sup>rd</sup> Floor

New York, NY 10271

Fax: 212-416-6003

Fax: 212-416-6042