



The Office Of State Treasurer
Denise L. Nappier

News

FOR IMMEDIATE RELEASE
December 9, 2013

CONSUMER ALERT: PROTECTING PERSONAL FINANCIAL INFORMATION

HARTFORD, CT – State Treasurer Denise L. Nappier today encouraged holders of prepaid debit cards issued by JPMorgan Chase, who may have been affected by a security breach with the bank's servers, to take precautions to ensure that no unauthorized activity has occurred on any of their accounts.

Personal information associated with certain debit cards may have been exposed between mid-July and mid-September during the course of an attack on the bank's servers which support its UCard website.

According to JPMorgan Chase, the breach affected cardholders in multiple states, including 14,335 accounts in Connecticut. The Connecticut accounts are prepaid debit cards issued by the State's Department of Revenue Services (DRS); Department of Labor; Department of Social Services; and Department of Children and Families. These cards are issued in place of checks to provide payments such as tax refunds, unemployment benefits or child support payments.

JPMorgan Chase is writing to affected cardholders in Connecticut, explaining what personal information may have been compromised and asking that accounts be closely monitored. The bank also will offer the affected cardholders free credit monitoring for two years.

In the meantime, Treasurer Nappier advised cardholders to:

- Scrutinize their financial accounts, including bank and credit card accounts, to check for any activity that they did not authorize.
- Take advantage of JPMorgan Chase's offer of two years of credit monitoring free of charge. Cardholders need to sign up for the service. Information on how to enroll will be provided in the notice that the company is sending to affected cardholders.

- Monitor their JPMorgan Chase prepaid debit card accounts and call the number on the back of their card if they see activity on the card that is not theirs, including withdrawals and purchases they do not recognize.
- Check their other bank accounts, because bank information may have been exposed if they transferred funds from their card to another account.

In addition, state residents should be wary of any callers offering credit or identity theft protection services, as such calls may be an attempt to elicit private consumer information.

“The unfortunate truth is that when events like this happen, it can bring out the criminal element. Identity thieves will use any tactic they can to steal your information, including capitalizing on people’s fears after a security breach,” said Treasurer Nappier.

No employee of a State of Connecticut agency will initiate a call telling a resident that his or her information is at risk and seeking personal financial information, and JPMorgan Chase will call only if they detect something suspicious and wish to confirm banking activity. Any calls asking for social security numbers, banking information or other personal information should be ended immediately and reported to authorities.

Residents who receive a suspicious call should report it to the Department of Consumer Protection’s Fraud Division at 1-800-842-2649 or DCP.Frauds@ct.gov.

"The Credit Union League of Connecticut appreciates the efforts of the Treasurer and her office in alerting and protecting consumers from this breach. We reiterate that any call telling a resident that his or her information is at risk should be ended immediately and reported to authorities," said Jill Nowacki, President & CEO - Credit Union League of Connecticut.

If you are concerned about identity theft, contact one of the three national credit reporting bureaus and ask them to look for suspicious activity. Individuals are entitled to one free credit report a year. More information is available at www.annualcreditreport.com.

The State’s Smart Consumer website, www.smartconsumer.ct.gov, has additional information on how to protect oneself from identity theft, and what to do if you suspect identity theft.

###