

**PRIVILEGED AND CONFIDENTIAL
FAX**

The Western Union Company
.....

Confidentiality Notice: The information transmitted, including any content in this communication is confidential, is intended only for the use of the intended recipient, and is the property of the Western Union Company or its affiliates and subsidiaries. If you are not the intended recipient, you are hereby notified that any use of the information contained in or transmitted with the communication or dissemination, distribution, or copying of this communication is strictly prohibited. If you have received this communication in error, please immediately return this communication to the sender and delete the original message.
.....

Date: September 6, 2006

**To: CPB
Security Breach Notification**

Fax No.: 518-474-2474

**From: James Keese
VP Privacy, Global Privacy Office**

Re: Reporting Form

Reporting Form
For Business, Individual or NY State Entity reporting a
"Breach of the Security of the System"
Pursuant to the Information Security Breach
and Notification Act (General Business Law §889-aa;
State Technology Law §208)

Name of Business, Individual or State Entity: **Western Union Financial Services, Inc.**
Date of Discovery of Breach: **August 11, 2006**
Estimated Number of Affected Individuals: **Nine (9)**
Date of Notification to Affected Individuals: **August 18, 2006**
Manner of Notification: written notice
 electronic notice (email)
 telephone notice

Are you requesting substitute notice? Yes No (If yes, attach justification)

Content of Notification to Affected Individuals: Describe what happened in general terms and what kind of information was involved. Please attach copy of Notice.

Back-up computer disks containing subscriber information related to the Western Union® Equity Accelerator® Program from the years 1999 through 2002 were stolen during a burglary in September 2005 from a storage facility belonging to Paymap, Inc. Paymap collects and maintains data under its contract with Western Union to provide processing and administrative services in support of the Program. Information on the disks may have included name, address, telephone number, Social Security number, loan account number(s), bank account information, a copy of the consumers' signature and copies of voided or cleared personal checks. Although the burglary occurred in September 2005, Paymap became aware of the potential data security breach, when contacted by the U.S. Postal Inspector, San Francisco Office on August 11, 2006. Western Union provided notification to effected individuals on August 18, 2006. To the best of our knowledge, the burglary was committed by a single individual who was not an employee of and is in no way connected to Western Union or Paymap.

A copy of the notification sent to affected individuals is attached.

Name of Business or Individual Contact Person: **James M Keese**
Title: **VP Privacy, Global Privacy Officer**
Telephone number: **720-332-3443**
Email: **jim.keese@firstdatacorp.com**

Dated: **September 5 2006**
Submitted by: **James M Keese**
Title: **VP Privacy, Global Privacy Officer**
Address: **12500 E. Belford Ave**
Email: **jim.keese@firstdatacorp.com**
Telephone: **720-332-3443** Fax: **720-332-0214**

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

Fax this form to:

CPB:

Security Breach Notification-

Fax: 518-474-2474

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

30 South Pearl St.

Floor P2

Albany, NY 12207

Fax: 518-474-9090

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

Attorney General:

Asst. Attorney General in Charge

Bureau of Consumer Frauds

120 Broadway - 3rd Floor

New York, NY 10271

Fax: 212-416-6003



P.O. Box 191090
San Francisco, CA 94133

August 18, 2006

[Consumer]
[1234 Street]
[City, State Zip]

Re: Important Information Regarding Your Privacy and your Equity Accelerator® Program Subscription

Dear [Consumer]:

We are writing to inform you of a recently discovered security incident at Paymap Inc. involving unauthorized access to your sensitive personal information. The incident was the result of a burglary at a Paymap secure storage facility in September 2005. Paymap collects and maintains your data under its contract with Western Union to provide processing and administrative services in support of your participation in the Western Union® Equity Accelerator® Program. We recommend that you review the information provided in this notice to protect yourself against any potential misuse of your personal information.

Computer disks containing Equity Accelerator® subscriber information from the years 1999 through 2002 were among the items stolen. Information on the disks may have included your name, address, telephone number, Social Security number, loan account number(s), bank account information, a copy of your signature and copies of your voided or cleared personal checks. To the best of our knowledge, the burglary was committed by a single individual whom was not an employee of and is in no way connected to Paymap or Western Union.

At the time, Paymap's search of the facility and its inventory gave no indication that information related to you was accessed or stolen. Immediately after discovery of the crime, Paymap took steps to secure the facility and further removed all potentially sensitive information to a secure area at its main corporate facility in San Francisco.

Although the burglary occurred in September 2005, Paymap only recently became aware of the potential data security breach, when they were contacted by the U.S. Postal Inspector. In the course of an ongoing investigation, local police and postal inspectors confiscated a number of stolen items, including the Paymap computer disks. Paymap immediately began an internal investigation to determine if a data security breach occurred, and the extent thereof. Paymap then notified Western Union of the situation.

Please be aware that there are some actions that only you can take to protect yourself from the misuse of your information. First, since your banking information may be involved, we recommend that you closely monitor your bank account and immediately report any unauthorized withdrawals or other unauthorized activity to your banking institution.

To further protect yourself, we also recommend that you place a fraud alert on your credit files. A fraud alert lets creditors know to contact you before opening new accounts. You can place a fraud alert on your files and receive a free credit report by contacting any of the three national credit reporting agencies:

Experian	Equifax	TransUnion
888-397-3742	800-525-6285	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Review your credit reports carefully. Look for accounts that you did not open. Look for inquiries from creditors that you did not initiate. And look for personal information, such as home address and Social Security number, that is not accurate. If you see anything that you do not understand, immediately call the credit reporting agency at the telephone number listed on your report.

If you do find suspicious activity on your credit reports, you may also want to contact your local police or sheriff's office to file a police report of identity theft. Get a copy of the police report. You may need to give copies to creditors.

Even if you do not find any signs of fraud or suspicious activity on your reports, we recommend that you check your credit report every three months for the next year. Contact one of the credit agencies listed above to order your reports and to keep the fraud alert in place.

For more information on identity theft, we suggest that you also visit the Federal Trade Commission Internet site at www.consumer.gov/theft.

We understand that you may have concerns about this issue. To help, Paymap and Western Union have established a toll-free hotline that you may call with questions. That hotline number is **1-800-519-1942**.

Paymap deeply regrets this incident and any inconvenience that it may cause our customers. Consumer data protection is a high priority for Paymap and Western Union and we are actively working with the appropriate law enforcement agencies to prosecute those responsible for this theft to the fullest extent of the law. We can assure you that we are evaluating our data security procedures to help prevent similar incidents in the future.

Sincerely,

Michael Mulligan
Vice President, Operations – Paymap Inc.