**Identity Theft/ Junk Mail and How to Avoid**

**By Ravi Nanju, January 2011**

**Most of UN staff who come must be careful especially with social security numbers and using credit cards and disposing off statements and receipts. Here are a few tips to avoid a big headache as identity theft is a big thing going on now.**

**Identity Theft**

The early signs of identity theft―when someone fraudulently uses your name, Social Security number, or a credit card number. Bills don’t arrive as expected, or bills show up for credit cards you’ve never applied up for. You’re denied a credit card for no apparent reason or you start getting calls or letters about purchases you didn’t make.

Note: Do not carry social security cards or any information that has you date of birth, passport details unless needed. Do not email to anyone unless it is secure/encrypted and you know the party well enough.

Beware of using credit cards or Bank Check Cards online for hotel bookings or travel bookings unless they are reputed companies. Inform your credit card company if you are travelling outside your home base (New York).

As much as possible while travelling in these countries use travelers checks.

**What to do if Your Identity is Stolen**

If your identity is stolen The Federal Trade Commission recommends you immediately take these four steps:

Call one of the three credit reporting companies and place a fraud alert on credit reports associated with your Social Security number.

Have any account that has been tampered with or opened fraudulently closed immediately.

Contact the Federal Trade Commission and file an official complaint.

Contact your local police and/or the police department in the community where the identity theft took place and file a report.

Fraud alerts prevent more fraudulent accounts from being opened in your name. To place a fraud alert on your credit report, contact any one of the three major national credit reporting companies.

* Equifax, (800) 525-6285
* Experian, (888) 397-3742
* TransUnion, (800) 680-7289

Check your credit report carefully for inquiries from companies you haven’t contacted, fraudulent accounts, and debts on your accounts you can’t explain. Also check the report to see that all of your personal information is correct. After correcting your report, submit an Identity Theft Report (see below) with a cover letter explaining your requests.

Closing fraudulent accounts involves calling the fraud department of each company and following up in writing with copies of documents supporting your case. Send these letters by certified mail and keep all of the correspondences on file. Ask the companies for specific forms used for disputing such charges.

Filing a complaint with the FTC can be done online by calling 1-877-ID-THEFT, or by mail.

* Identity Theft Clearinghouse
* Federal Trade Commission
* 600 Pennsylvania Ave. NW
* Washington, D.C. 20580

Upon completing the report you will be issued an FTC ID Theft Complaint form.

A police report can be filed by your local police department. Ask to file the report in person, if possible. When filing the report, have your FTC ID Theft Complaint form,  and all supporting documents. Ask the officer for a copy of the Identity Theft Report.

**Identity Theft Reports**

An Identity Theft Report is essentially a very detailed police report including enough information about the crime for the credit reporting companies and the businesses involved to verify your claim. The police are not obligated to use the FTC ID Theft Complaint Form as part of their report and may have another way to incorporate the information. In such cases, the police report alone serves as an Identity Theft Report.

Send a copy of your Identity Theft Report along with a letter and copies of supporting documentation to the fraud departments of the three major credit reporting companies. Send the same information to all the companies that have been defrauded in your name.
Filing an Identity Theft Report will block fraudulent information form appearing on your credit report and should prevent fraudulent debts from reappearing. It also works to prevent companies from collecting or sending to collections debts that are the result of identity theft. Be advised, the credit reporting companies can deny your Identity Theft Report if it is not detailed enough, and may request addition information.

**Identity Theft and the DMV**

If you suspect that your name or Social Security number are being used to obtain a fraudulent driver’s license or state ID, contact your state Department of Motor Vehicles. If your state uses your Social Security number as your license or ID number you can request to substitute another number.

While many cases of identity theft start with mail containing personal information being stolen from mailboxes or garbage bins, losing a wallet or purse can give thieves access to the same information. While visiting the DMV, make sure to keep track of your belongings at all times.

**Prevention**

These are some of the things the FTC recommends doing to prevent identity theft.

* Watch your Social Security Number like a hawk. If someone asks for it, find out how it will be used, how it will be stored and how it will be protected. Don’t carry your Social Security card on your person, keep it stored securely at home.
* Watch what you throw away. Identity thieves love digging through garbage for sensitive information, so it’s best to shred the following documents: charge receipts, copies of credit applications, insurance forms, physician statements, checks and bank statements, expired charge cards, and credit offers.
* Be careful what personal information you release while using the Internet safely.
* When creating passwords for credit card, bank, and phone accounts, combinations of letters, numbers, and special characters make the strongest passwords, as opposed to those relating directly to personal information, such as pet names and birthdays.
* Always make sure you know exactly who it is that you are giving personal information to, whether over the phone or the Internet.
* Every year you can get a free copy of the credit report form all three agencies for free from [www.ftc.gov](http://www.ftc.gov/)
* Also register free at [www.ftc.gov](http://www.ftc.gov/) to remove your name from being shared by marketing companies and flooding you with junk mail.
* Do not give your telephone number when you pay by credit card at any store here as they data mine you and get the address and send you junk mail.
* If you want to receive offers give a **new email id** which you use only for this purpose and  receive and open offers that you want to.
* When applying for cell phones go to company stores where your personal information I secure and not shared. Small mom and pop stores use your social security numbers to open new prepaid accounts that they sell to non immigrants or those not eligible to get a cell phones SIM card. Most college students on arriving in New York get prepaid cell phones that quite often is dubious as someone else’s social is being used.
* ***If leaving the country for good write a letter to social security and send back the card using a registered mail so that you have proof. This was your number is not misused and you have no liability.***