



UBS Financial Services Inc.
1000 Harbor Boulevard
Weehawken, NJ 07086

Dennis Dickstein
Chief Privacy Officer
dennis.dickstein@ubs.com
201-352-4933

September 9, 2008

Via Express Mail

Martha Coakley, Esq.
Attorney General
Office of the Attorney General
McCormack Building
One Ashburton Place
Boston, MA 02108

Daniel Crane, Director
Massachusetts Office of Consumer Affairs and Business Regulation
Ten Park Plaza, Suite 5170
Boston, MA 02116

Dear Ms. Coakley and Mr. Crane:

I am the Chief Privacy Officer of UBS Financial Services Inc. Pursuant to ALM GL ch. 93H Section 3, I am writing to inform you of the following:

On August 11, 2008, UBS IT Risk Control was informed by a vendor that two spreadsheets containing sensitive UBS information had been identified on a peer-to-peer file sharing network. UBS immediately began researching the source of this data leakage and determined that a Human Resources employee had e-mailed these documents to a personal computer outside of UBS on July 15, 2008 to work on them prior to leaving for vacation. The personal computer that received this e-mail contained file sharing software for a peer-to-peer network. To date, UBS has received no report of unauthorized use of the data contained in the spreadsheets.

These spreadsheets contained information relating to 1,744 current or former UBS employees that participated in or applied for acceptance to our tuition reimbursement program. Our current information indicates that the affected UBS personnel are residents of 49 states, with 56 being Massachusetts residents. The data elements contained in the spreadsheet are the following: (i) Last Name; (ii) First Name; (iii) Social Security Number; and (iv) School and Declared Major.

While we are not aware of any evidence that the information has been misused by an unauthorized person, we provided written notice to the UBS employees to alert them of this incident on September 9, 2008. We have also provided an Identity Theft Prevention Fact Sheet and a toll free number to call with any questions. In addition, we have taken steps to ensure that the spreadsheets have been removed from the employee's personal computer, have begun an initiative to reduce the instances where employee social security numbers are stored and used and install new protections for cases where the information is required.

Should you have questions, please do not hesitate to contact me.

Sincerely,

A handwritten signature in black ink that reads "Dennis Dickstein".

Dennis Dickstein
Chief Privacy Officer



UBS Financial Services Inc.

1000 Harbor Boulevard
Weehawken, NJ 07086

Dennis Dickstein
Chief Privacy Officer
dennis.dickstein@ubs.com
201-352-4933

September 18, 2008

Scott D. Schafer
Deputy Division Chief – Consumer Protection Division
Office of the Attorney General
McCormack Building
One Ashburton Place
Boston, MA 02108

Dear Mr. Schafer:

I am in receipt of your correspondence dated September 12, 2008 regarding our notification of a data security breach. As requested, I have enclosed a copy of the notice that was provided to Massachusetts residents pursuant to ALM Gl ch. 93H, §3. However, I would like to clarify that our notification letter did not reference a Massachusetts resident's right to obtain a police report since we did not consider this a criminal matter, and therefore, did not file a police report.

Should you have questions, please do not hesitate to contact me.

Sincerely,

A handwritten signature in black ink that reads "Dennis Dickstein".

Dennis Dickstein
Chief Privacy Officer

Enclosure



UBS Financial Services Inc.
1000 Harbor Boulevard
Weehawken, NJ 07086

Dennis Dickstein
Chief Privacy Officer

www.ubs.com

September 9, 2008

Dear current or former UBS employee,

I am writing to inform you of a recent incident that might involve unauthorized access to your personal information. We take our obligation to protect the privacy of personal information very seriously and deeply regret that this incident occurred.

Although we have no reason to believe that information about you has been misused, we are notifying you about this incident so that you may monitor, if you choose, the use of personal information and take action in the event of potential misuse of such information.

Enclosed is a fact sheet that outlines steps you can take to protect yourself, including adding free fraud alerts to your credit files, reviewing free annual credit reports, and utilizing security freezes. We encourage you to review this fact sheet and to always monitor your credit reports and remain vigilant about fraud and identity theft.

Once again, we regret that this situation occurred and we appreciate your understanding. If you have any questions, please contact the UBS Financial Services Inc. Service Center at 800-251-7014. This dedicated toll-free phone line has been set up specifically for calls regarding this incident and will be available Monday through Friday from 9:00 a.m. – 5:00 p.m., Eastern Time, until November 7, 2008. You also may e-mail the WMA Privacy Office at Privacyoffice@ubs.com.

Sincerely,

A handwritten signature in black ink that reads "Dennis Dickstein".

Dennis Dickstein
Chief Privacy Officer

Enclosure

FACT SHEET – STEPS TO HELP PROTECT AGAINST IDENTITY THEFT

Fraud Alerts

A fraud alert is free. A fraud alert would tell current and potential creditors checking your credit file that either: a) recent fraudulent activity has taken place, or b) you are fearful that fraudulent activity may take place in the future. A potential creditor would then know to contact you before opening new accounts. A fraud alert is displayed for 90 days and may be extended up to seven years with submission of an identity theft report. You may place a fraud alert on your credit files at the three major consumer reporting agencies by contacting any one of them at the numbers below:

Experian
888 397-3742

Equifax
800 525-6285

TransUnion
800 680-7289

When you place a fraud alert in your credit file, the consumer reporting agencies will inform you of your right to request a copy of your credit report at no charge. (Note that you also have the right to obtain a free credit report annually independent of a fraud alert by contacting www.annualcreditreport.com). When you receive your credit reports, look them over carefully for: accounts you did not open; inquiries from creditors that you did not initiate; and personal information, such as home address or social security number that is not accurate. If you see anything you do not understand, call the consumer reporting agency at the number on the report.

If you find suspicious activity on your credit reports, file a police report. Request a copy of the police report, because many creditors want the information it contains to absolve you of any fraudulent debts. You also should file a complaint with the Federal Trade Commission at www.consumer.gov/idtheft or at 1-877-IDTHEFT (1-877-438-4338). Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. Close the accounts that you know or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit when disputing new unauthorized accounts. You may also wish to contact your credit card issuers and financial institutions and inform them of the incident. In addition, you may contact the fraud departments of the three major consumer reporting agencies listed above to further discuss your options.

Even if you do not find any signs of fraud, we recommend that you check your credit report every three months. Just call one of the numbers above in the Fraud Alerts section to order your reports and keep the fraud alert in place. For more information about identity theft, contact the FTC at the telephone number or website listed above.

Security Freeze

Under Massachusetts law you have the right to place a security freeze on your credit file. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent; however, using a security freeze may delay your ability to obtain credit. You may request that a security freeze be placed on your consumer report by sending a request to a consumer reporting agency by certified mail, overnight mail or regular stamped mail to the address below. The following information should be included when requesting a security freeze (documentation for both the spouse and the victim of identity theft must be submitted when requesting a security freeze for the spouse): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past two years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request also should include a copy of a government issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent).

The consumer reporting agency may charge a reasonable fee of up to \$5.00 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a police report relating to the identity theft to the consumer reporting agency.

Equifax Security Freeze

PO Box 105788

Atlanta, Georgia 30348

http://www.equifax.com/cs/Satellite?c=EFX_ContentRoot&cid=1165203975981&pagename=5-1%2F5-1_Layout

Experian

PO Box 9554

Allen, TX 75013

http://www.experian.com/consumer/security_freeze.html

TransUnion

Fraud Victim Assistance Department

PO Box 6790

Fullerton, CA 92834

<http://www.transunion.com/corporate/personal/fraudIdentityTheft/preventing/securityFreeze.page>