2024-573

UBS Financial Services Inc.
One Post Office Square
Boston, MA 02109

Tel. +1-617-439-8000
www.ubs.com

March 21, 2024

[redacted]

RE: UBS Financial Services Inc. Account and Online Services

Dear [redacted]

We are writing to notify you of a breach of security at UBS Financial Services Inc ("UBS") that occurred on February 7, 2024 ("Security Breach"). The Security Breach included your account number and, subsequently, your contact details, such as email and home address. Your social security number was not included in the Security Breach. Additionally, in the course of investigating the Security Breach, UBS FSI determined that your social security number or at least its masked form (i.e., the last 4 digits), your name and your date of birth were already affected by a previous unauthorized acquisition and were in use by other actors, both unrelated and unaffiliated with UBS FSI.

Following the Security Breach and discovery of the unauthorized acquisition and use, the following security measures have been put in place:

- ✓ E99 FB0 security flag[1] is maintained (which was first put in place in October 2023),
- ✓ Your account number was changed, and
- ✓ Your Online Services business account was locked.

Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Massachusetts law also provides that, in case of a breach of security including a social security number, a subscription to a service to help monitor, detect, and alert you about potential privacy threats of a duration not shorter than 18 months should be provided to you at no cost. Even though your social security number was not included in the breach, we have decided to make such services available to you in order to aid you in securing your personal information and your financial assets. We have attached a copy of the UBS Identity Protection Factsheet (Factsheet) which provides

[1] An E99 FB0 security flag is added to an account when there was a possibility of or concern about a compromise of personal information or an identity theft.

UBS

information on how to apply for the service of your choice. UBS will reimburse the costs of the service you have incurred. By the time you have received this letter, the above procedures might also have been explained to you by an UBS FSI branch representative.

In addition, it is always a good practice to be vigilant and closely review and monitor your financial accounts, statements, credit reports from the three major credit reporting agencies, and other financial information for any evidence of unusual activity, fraudulent charges, or signs of identity theft. We strongly suggest that you review the enclosed Factsheet as it includes additional actions that you may wish to take to further safeguard your personal information, including recommendations from the Federal Trade Commission, and it provides details regarding placing a fraud alert or free security freeze on your credit file. We urge you to carefully review this document and consider taking the actions contained therein. Also, we invite you to peruse the provided Cybersecurity Checklist for further advice on safeguarding your data.

For more information on identity theft, fraud alerts, security freezes and obtaining your credit reports you can refer to the enclosures and visit the following websites:

- Massachusetts Attorney General at: https://www.mass.gov/reporting-data-breaches
- Federal Trade Commission at: www.ftc.gov/bcp/edu/microsites/idtheft/

If you have any questions or concerns, please contact me directly. You may also contact the UBS Data Protection Office at DPO-US@UBS.com.

We assure you that we take the protection of your personal information very seriously and regret any inconvenience this incident may have caused.

Sincerely,

Lili M. Trudeau
Supervisory Officer
617-439-8517
lili.trudeau@ubs.com

cc: Timothy Gray

UBS

Protecting yourself against identity theft

Some steps you can take to manage your risk

Identity theft (or identity fraud) occurs when an impostor obtains and uses key pieces of personal information, such as name, address, Social Security number, credit card or bank account information, without permission, to impersonate another person for illegal financial gain or some other illicit benefit. If this happens to you, it can impact your finances as well as other aspects of your life. Therefore, it is important for you to be aware of the measures that you can take, as needed, to help to protect yourself against such risks.

Place a fraud alert on your credit files

If you are concerned that your personal or financial information has been compromised or misused, you can place a fraud alert on your credit files by contacting *any one* of the 3 national consumer reporting agencies listed below. A fraud alert is free and will require a business to contact you if someone tries to open a new account in your name or before the business issues credit to someone using your name. A fraud alert will initially be displayed for 1 year (and may be extended up to 7 years if you file an identity theft report with the Federal Trade Commission (FTC)).

Once a fraud alert is placed, you will be entitled to request a free copy of your credit reports directly from the 3 national consumer reporting agencies. You also have the right to obtain free copies of your credit reports annually and independent of a fraud alert through *annualcreditreport.com* or by calling 877-322-8228.

Use a security freeze

If your personal information has been compromised or you notice suspicious activity on your credit reports or on other account statements, you may also want to place a security freeze (also known as a credit freeze) on your credit reports, which is available free of charge.

A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. This can also help to prevent an impostor from opening a new account in your name without your knowledge. Bear in mind that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. Under federal law, you cannot be charged to place, lift, or remove a security freeze.

This must be done individually with *each* of the 3 national consumer reporting agencies (refer to the phone numbers/addresses listed below).

Review your credit reports carefully

When you receive your credit reports, read through them carefully and look out for any information that appears incorrect, unusual, or out of the ordinary, such as:

- unfamiliar accounts or charges;
- inquiries from creditors that you did not initiate;
- claims made by creditors that you are not aware of; or
- any inaccuracies in your personal information, such as home address or Social Security number.

If you find any errors or wish to dispute any item, you should notify that consumer reporting agency and the information provider that is shown on your credit report.

Even if you do not find any indications of fraud or misuse of your information, it is still prudent to routinely review your credit reports.

National Consumer Reporting Agencies

Experian	Equifax	TransUnion
888-397-3742	888-766-0008	800-680-7289
experian.com	equifax.com	transunion.com

Notify relevant authorities and interested parties
You should consider filing a police report if your personal information has been misused or if you find fraudulent activity in your credit report. Remember to keep a copy of the police report for your records, so that you can provide it to creditors when disputing any claims or debts resulting from identity theft.

You can also file an identity theft report with the Federal Trade Commission (FTC) at *identitytheft.gov* or by calling 877-IDTHEFT (877-438-4338). Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement to facilitate investigations and prosecution of identity theft.

If you suspect that your Social Security number and other personal information have been compromised or used fraudulently, you may want to review the taxpayer guidance provided by the Internal Revenue Service (IRS) at https://www.irs.gov/newsroom/taxpayer-guide-to-identity-theft or call them at 800-908-4490 to discuss potential protections for your next tax return, such as filing an Identity Theft Affidavit (Form 14039).

Lastly, you might want to inform your bank, financial institutions and other key contacts with whom you do business to alert them of your identity theft concerns so that they can take the appropriate precautions such as having security flags added to your accounts, changing your account numbers or closing inactive accounts or accounts that you believe have been tampered with or opened fraudulently.

Sign up for identity theft protection products or services
UBS Visa Infinite credit cardholders have access to both a Personal Identity Theft coverage benefit and an Identity Theft Resolution Services benefit. Cardholders should contact UBS Client Services at 888-762-1232 for additional information.

There are different vendors that provide various types of identity theft protection products and/or services to the public, some of which offer features that extend beyond basic credit monitoring. Many of these vendors charge a fee for their products and services. These vendors can also provide identity theft related guidance. You may want to investigate what products and/or services are available in the market and decide what is appropriate for you, and the level of protection you need. Some well-publicized vendors are:

Company	Telephone	Website
AllClear ID	855-434-8077	*allclearid.com*
Equifax	866-243-8181	*equifax.com*
EverSafe	888-575-3837	*eversafe.com*
Experian	888-397-3742	*experian.com*
Identity Guard	833-692-2187	*identityguard.com*
LifeLock	800-416-0599	*lifelock.com*
TransUnion	877-322-8228	*transunion.com*

Some vendors may offer discounts to UBS clients. Please check with vendors directly to determine if a discount is available to you.

UBS Financial Advisors are not permitted to serve as a client's representative or advocate (i.e., a "trusted advocate" as described by EverSafe) relating to products and services offered by the companies listed above and other companies providing similar products and services.

Be vigilant and aware
As criminals grow increasingly sophisticated and creative in how they commit identity theft, fraud, and other related criminal activities, it is important for you to keep yourself up-to-date and informed about these matters. For example, the FTC, the 3 national consumer reporting agencies, and many states' Attorneys General or Departments of Consumer Affairs provide useful information through their websites on how to prevent, respond to, and/or mitigate risks associated with identity theft.

UBS

Cybersecurity

Protect your identity in the digital age

Follow these steps to minimize your risk of becoming a victim of cyber-crime.

Cyber fraud has increased exponentially over the last few years and it is no longer a question of whether you'll be targeted by cybercriminals, but when. It is important that you are prepared and protect yourself as much as possible from this growing threat.

E-mail compromise 	This is when your e-mail or an associates' e-mail is spoofed or hacked and used to trick you or your bank into making a payment.
Viruses 	Malicious programs that attach themselves to authentic programs and run without permission on your computer or device.
Social engineering 	This is when criminals convince you to provide your personal or financial information under false pretenses, often by posing as someone else.
Phishing 	This is when cybercriminals use e-mail to try to lure you into revealing your personal or confidential information by clicking a link or an attachment.
Identity theft 	The unauthorized acquisition and use of someone's personal information, usually for financial gain.
Ransomware 	A malicious program that blocks access to your computer, device or data, and demands that you pay a ransom to regain access.

Key action steps

- Make sure you always stop and consider each e-mail you receive and call back the sender on a known number if something seems unusual or pressured in the request.
- Avoid opening e-mails from unknown senders, downloading unexpected attachments or clicking on unfamiliar links.
- Use strong passwords and avoid sending personal or confidential information on unsecured networks.
- Secure your computer and devices by installing security patches and anti-virus protection.

Business E-mail Compromise (BEC)—E-mail requests for order placing of fund transfers

- A fraudster impersonates your business partner's e-mail (e.g., JoeVVright@gmail.com as supposed to JoeWright@gmail.com) and sends a last minute request for you to make a payment to another bank account.
- Rather than responding to the e-mail request, use an alternative channel or known contact number to verify the request.

Tech Support Scam (e.g. Acting as Microsoft Tech Support)

- A current live scam that is prevalent globally relates to fraudsters spoofing the incoming telephone to appear to be the official tech support team of a reputable tech company. The bad actor then uses social engineering skill to install malware and hijack your e-banking account to disburse payment(s),

Browse the web and check e-mail securely

- ☐ Avoid using public computers or Wi-Fi hotspots when sending personal or confidential information
- ☐ Only shop with reputable online vendors, and use credit cards or PayPal (not debit cards)
- ☐ Be careful about what personal information you make publicly available and send it only on secure websites ("https")
- ☐ Learn to recognize phishing; never open unfamiliar attachments or click on unfamiliar links
- ☐ Ignore e-mails or text messages that ask you to confirm or provide personal information by replying to the e-mail or message
- ☐ Use the filtering settings on your internet browsers and search engines

Manage your social media activities

- ☐ In your profiles and posts, avoid publishing personal information that is typically used for security or verification purposes, such as your full birthdate or your mother's maiden name
- ☐ Use privacy settings to control who can access your information, and review your privacy settings regularly
- ☐ Accept friend requests only from people you know; only "follow" (not "friend") entities or public figures
- ☐ Be wary of sharing your current location or future travel plans; never announce when you won't be home
- ☐ Be careful about taking online polls or quizzes or downloading apps that allow the organizer to access your account or data on your devices

Strengthen your passwords

- ☐ Create passwords that are at least 6 to 15 characters long
- ☐ Use a combination of special characters, numbers and upper and lower case letters, passphrases or password managers
- ☐ Avoid including personal identifiers, such as names or birthdates, in your passwords
- ☐ Store your passwords securely and change them regularly, at least once every 3 – 6 months
- ☐ Do not use the same password for all of your accounts
- ☐ Use multi-step authentication procedures whenever possible
- ☐ Do not allow "auto-save" of your passwords

Protect your computer and devices

- ☐ Use a strong password and biometrics when available to access your devices
- ☐ Set your computer and devices to auto-lock after a short period of inactivity
- ☐ Set all computers and devices for automatic software updates
- ☐ Install up-to-date security software with anti-virus, anti-malware and identity protections
- ☐ Avoid keeping financial and confidential information on your devices unless necessary
- ☐ Use file encryption for personal information that must be stored on your devices
- ☐ Keep a copy of critical data on a separate, secure medium (e.g., an encrypted external hard drive)
- ☐ Do not allow text messages or caller ID to appear on your locked screen
- ☐ Make sure you completely erase your hard drives prior to disposal
- ☐ Make sure that an owner's permission and password is required to access your home Wi-Fi network and that it is password protected and secure
- ☐ Create a security PIN to access your device
- ☐ Turn off location services and unnecessary apps on your devices
- ☐ Do not store or send personal or confidential information via e-mail or text
- ☐ Monitor your phone for unusual activity (texts you did not send, unusual pop ups or higher than normal battery usage)

Monitor financial statements and credit reports

- ☐ Request and review credit reports from each of the three national consumer reporting agencies regularly
- ☐ Review your bank and credit card statements regularly, and look out for suspicious activity or unfamiliar charges
- ☐ Review your Social Security Administration records annually
- ☐ Go through your health claims carefully to ensure you've received the care for which your insurer paid
- ☐ Remove your name from marketing lists, including for the three credit reporting bureaus (Experian, Transunion, Equifax), to prevent unsolicited credit offers
- ☐ Sign up for identify theft protection products or services, as appropriate for you
- ☐ Place a fraud alert on your credit files if you are concerned that your personal or financial information has been compromised or misused
- ☐ Freeze your credit to block new credit cards, loans or credit lines being opened without your consent