Lakeside Advisors, Inc.
Privacy Statement

Lakeside Advisors, Inc.
1115 East Denny Way
Seattle, WA 98122

Lakeside Advisors, Inc., an independent investment management firm, is committed to safeguarding the confidential information of its clients. We hold all personal information provided to our firm in the strictest confidence. These records include all personal information that we collect from you in connection with any of the services provided by Lakeside Advisors, Inc. We have never disclosed information to nonaffiliated third parties, except as permitted by law, and do not anticipate doing so in the future. If we were to anticipate such a change in firm policy, we would be prohibited under the law from doing so without advising you first. As you know, we use health and financial information that you provide to us to help you meet your personal financial goals while guarding against any real or perceived infringements of your rights of privacy. Our policy with respect to personal information about you is listed below.

- We limit employee and agent access to information only to those who have a business or professional reason for knowing, and only to nonaffiliated parties as permitted by law. (For example, federal regulations permit us to share a limited amount of information about you with a brokerage firm in order to execute securities transactions on your behalf, or when you have authorized our firm to discuss your financial situation with your accountant or lawyer.)
- We maintain a secure office and computer environment to ensure that your information is not placed at unreasonable risk.
- The categories of nonpublic personal information that we collect from a client depend upon the scope of the client engagement. It will include information about your personal finances, information about your health to the extent that it is needed for the planning process, information about transactions between you and third parties, and information from consumer reporting agencies.
- For unaffiliated third parties that require access to your personal information, including financial service companies, consultants, and auditors, we also require strict confidentiality in our agreements with them and expect them to keep this information private. Federal and state regulators also may review firm records as permitted by law.
- We do not provide your personally identifiable information to mailing list vendors or solicitors for any purpose.
- Personally identifiable information about you will be maintained during the time you are a client, and for the required time thereafter that such records are required to be maintained by federal and state securities laws, and consistent with the CFP Board Code of Ethics and Professional Responsibility. After this required period of record retention, all such information will be destroyed.

We maintain a Business Continuity Plan describing how we intend to respond in the event of Significant Business Disruptions due to natural disaster, technology failure, or terrorist activity. Our Business Continuity Plan is available upon request or at www.lakesideadvisors.com

We routinely suggest to our clients that they be vigilant in reviewing their credit and overseeing their financial transactions, and want to take this opportunity to reiterate this recommendation. Attached is an explanation of additional steps you may want to consider to protect against fraud and identity theft.

Identity Theft Precautions

1. Fraud Alert

As a precaution against identity theft, you can consider placing a fraud alert on your credit file. A "fraud alert" tells creditors to contact you before they open any new accounts or change your existing accounts. A fraud alert also lets your creditors know to watch for other unusual or suspicious activity. To place a fraud alert, call any one of the three major credit bureaus, listed below. An initial fraud alert remains effective for ninety days, and is free of charge. If you wish, you can renew the fraud alert at the expiration of this initial period. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file.

2. Security Freeze

You can also consider placing a security freeze on your credit reports. A "security freeze" prohibits a credit reporting agency from releasing any information from your credit report without written authorization. Placing a security freeze on your credit report may delay, interfere with, or prevent timely approval of requests you make for new loans, credit mortgages, employment, housing or other services; therefore, take time to consider the benefits and potential drawbacks of a security freeze.

If you have been a victim of identity theft and you provide the credit reporting agency with a valid police report, the agency cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit reporting agency may charge you a fee to place, temporarily lift, or permanently remove a security freeze. The cost to place, lift, or remove a credit freeze varies depending on the state you live.

To place a security freeze on your credit report, you must contact **each** of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. The contact information for the three major consumer agencies is provided below:

Equifax Security Freeze
P.O Box 105788
Atlanta, GA 30348
Phone: 800-685-1111
www.freeze.equifax.com

TransUnion Security Freeze
Mail: TransUnion LLC
P.O. Box 2000
Chester, PA 19016
Phone: 888-909-8872
freeze.transunion.com

Experian Security Freeze
Regular Mail: P.O. Box 9554
Allen, TX 75013
Overnight Mail: Experian
711 Experian Parkway
Allen, TX 75013
Toll-free: 888-397-3742
www.experian.com/freeze

In order to request a freeze, you will need the following information:

1. Your full name.
2. Proof of current address such as a current utility bill or telephone bill.
3. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years.
4. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
5. Date of birth.
6. Social Security Number.
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.
8. If you are not a victim of identity theft, include payment for the service.

After receiving your request, the credit bureaus will send a written confirmation to you and provide you with a unique personal identification number (PIN) or password (or both). You will use this PIN (or password) to lift the security freeze in order to allow a specific entity or individual access to your credit report, and to remove the security freeze.

3. Further Information

You may obtain additional information by contacting the Federal Trade Commission (FTC) or visiting the FTC's privacy and identity theft website, as follows:

FTC identity theft phone line: 1-877-IDTHEFT (438-4338)
FTC identity theft website: www.consumer.ftc.gov/topics/identity-theft

Mom's Maiden Name? The Right Way to Answer Security Questions and More Online Safety Advice

After Yahoo's record-setting security breach, it's time to get smarter about account logins

Massive online security breaches have troublingly become routine, and Yahoo Inc.'s latest raises the bar, compromising more than one billion accounts. While some hacks are beyond your prevention, it's a stark reminder that you need to try to stay one step ahead of the hackers.

Better security answers

You need to be careful when answering security questions. Usually, you're asked questions such as the name of your elementary school, your mom's maiden name or something related to a favorite sports team or movie.

Anyone can guess most of the answers to these things by a quick scan of your Facebook and LinkedIn profiles. Instead of the same old answer, take a different tack.

You can spell the answer backward. You can write the answer in a different language. You can write the answer in the form of a question. Consider adding symbols (such as a #, $ or % character) or a capital letter at the beginning and end of answers, or in place of spaces.

If you always use a capital Z in place of a space and you write your answers backward, you'll remember your unique approach across your online life, regardless of the answer.

One thing you might not want to do, however, is lie. We really only run into these questions when we set up our online accounts and when we forget our passwords or need to reset them. If your answer is a lie, then you might forget what the lie was.

Get into a routine

Protecting yourself online might seem like a lot of work, so make a routine out of it. If you ask yourself to do this sort of thing weekly, you won't do it. Try a quarterly schedule to start. That's a frequent enough pace to be safe, but also slow enough that we can stick to it."

Add something like "online security check" to your calendar every three months, on a day off for which you know you'll be able to make the time. This is when you can use a password manager, an app such as Dashlane that securely stores passwords and other login information.

Don't be afraid to walk away

Use your checkup as an opportunity to consider deleting accounts you don't often use, or are uneasy about using in the future.

The record-setting Yahoo attackers used Yahoo's own software to create its fake user credentials that circumvented two-factor authentication security measures. "Since the attackers were using Yahoo's own code, you could change your password 100 times and it wouldn't matter.

Yahoo has repeatedly been the victim of attacks. With little reassurance that things will change, it makes sense to choose a competitor, such as Gmail or Microsoft Corp.'s Outlook.com. If you depend on Yahoo for fantasy sports, ESPN and most sports leagues offer alternatives. Flickr's photo service now has many compelling alternatives, including Google Photos and Apple Photos.

Remember what's at stake here. This is sensitive personal information in context. A username, email address, phone number and date of birth can be found in many online accounts. As individual pieces of information, this is harmless. Yet combined, it can be more than enough for someone to pose as you online.