PRIVACY POLICY

Protecting your privacy is important to us at 20/20 Capital Management, Inc. We take precautions to ensure that your information is kept safe and remains private. To assist us in providing you the quality services and products that you request or to help meet your needs, we gather, maintain, and use both public and nonpublic personal information about you. We are providing you with the following statement describing our policies and practices with respect to sharing of customer information.

Facts	What does CMI do with your personal information?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information.
What?	We collect nonpublic personal information about you from the following sources: • Information we receive from you on applications and other forms • Information about your transactions with us, our affiliates, or others • Information you give us verbally • Social security number, DOB • Income information • Assets, holdings, transaction information "Nonpublic personal information" means personally identifiable financial and other related information that is not available from public sources. If your customer relationship with us terminates, or if you become an inactive customer, our privacy policy will continue to apply to you.
How?	All financial companies need to share customers' personal information to run their daily business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons CMI chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does CMI share?	Can you limit this sharing?
For our everyday business purposes *Such as process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus*	Yes	No
For our marketing purposes *To offer our products and services to you*	Yes	No
For joint marketing with other financial companies	No	No
For our affiliates' everyday business purposes *Information about your transactions and experiences*	Yes	No

For our affiliates' everyday business purposes *Information about your creditworthiness*	No	Yes
For affiliates to market to you	Yes	Yes
For non-affiliates to market to you	Yes	Yes

Questions or need more information?	Go to www.2020CMI.com or call 714-433-1299

Who we are

Who is providing this notice?	2020 CMI | 2020 FA and its affiliates

What We Do

How do 2020 CMI and 2020 FA protect my personal information?

We train our employees in the proper handling of personal information and oversee the same.

To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. All nonpublic personal (NPI) information is treated as strictly confidential and is not disclosed except to employees for the purpose of carrying out their responsibilities and to affiliated and nonaffiliated firms necessary to affect and administer custodial, brokerage, financial planning, legal, accounting, insurance or similar services requested and authorized by the client. Federal and state regulators also may review client records as permitted under law. 2020 CMI requires that our affiliates protect and restrict the use of client information. Several practices are presently in place to ensure private client information is secured from public access:

Secured Paper Files: Filing cabinets are locked outside of regular business hours. Paper shredders are utilized to dispose of papers that contain NPI client information. Sites of business are securely locked and multiple offices are electronically armed for fire and theft outside of regular business hours.

Secured Electronic Files, Databases and Systems: computer systems are secured by a password system and all workstations are logged-off or locked outside of regular business hours. Any electronic information accessible through the Internet is guarded by a firewall, and computers are scanned for viruses. Additional layers of protection include the use of threat monitoring software, use of encryption, VPN's, multifactor authentication, password managers to help enforce strong passwords and cyber education. Firm utilizes outsourced SEC compliant data governance electronic storage platform for back-ups of electronic data essential to its operations on a daily basis, with the prior day's backup encrypted and maintained at several remote locations in case of disaster.

E-mail: When associates correspond with clients regarding private or sensitive matters they are encouraged to communicate that information via an secure encrypted manner available for free to associates and clients. When sending electronic mail associates are educated to send using encrypted email methods. Disclosures are included in emails to help alert clients of phishing attempts and malicious links. E-mail communications to third parties which relate to our clients are conducted only as necessary to fulfill the obligations of the firm.

Other Internal Measures:
In addition to these measures, Firm and its employees avoid storing nonpublic personal information in plain view in areas where it may be seen by third parties or discussing such information in public places where it may be overheard.

External Security Measures (Security is a Partnership): We consider security to be a partnership between us and our clients. Taking some basic, preventative steps can help make your personal information more secure. Many involve plain common sense, like routinely checking your monthly statements to ensure reported account activity is legitimate. Other steps include:

	(1) Keep your computer equipment updated: • Keep your web browser and operating system updated and activate the computer firewall and encryption settings. If using Windows, we recommend Windows 10 Pro or newer. Old software and browsers can be susceptible to attack • Install anti-virus and anti-spyware software on all platforms (Windows, Apple and mobile devices). Your cable provider may provide free anti-virus software such as McAfee Security Suite at no additional charge. Check with your cable provider. • Check your security settings on your applications and web browser or with the help of a local IT professional or service (e.g. Geek squad or similar). • We recommend the use of a VPN at all times when communicating with associates of our firm. (2) Verify you are using a secure website. (3) Be extremely cautious if using public networks: • Be cautious when using public computers. If you do use one, clear the browser's history (cache) and cookies before leaving. • Only use wireless networks you trust or that are protected. Public Wi-Fi locations can be dangerous places to connect your devices. Pay attention to security warnings that pop up. Don't accept software updates when connected to a public Wi-Fi. • Use VPN at all times when using public network (4) Keep secure your login credentials & passwords: • Don't use personal information such as your birthday as part of your login ID. • Create a unique password for each financial institution you do business with and change it every six months. • Don't share your passwords. (5) Be alert to phishing and other scams: Beware of attempts to "phish" your information. These are often in the form of urgent-sounding emails where you might be encouraged to click on a link in order to update personal information. Even clicking on the link could potentially take you to a malicious website, where malware could infect your computer. We strongly recommend that you not click on any suspicious links.
How do 2020CMI and 2020FA collect my personal information?	We collect your personal information, for example, when you: • Open an account/policy • Seek advice about your investments/planning • Enter into an investment/planning advisory agreement • Tell us about your investment or retirement portfolio We also collect your personal information from others such as credit bureaus, affiliates, or other companies.
Why can't I limit all sharing?	Federal law gives you the right to limit only: • Sharing for affiliates' everyday business purposes – information about your creditworthiness. • Affiliates from using your information to market to you. • Sharing for non-affiliates to market to you. State laws and individual companies may give you additional rights to limit sharing. [See below for more on your rights under state law.]
Definitions	

Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. *2020 CMI | 2020 FA*
Non-Affiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies.
Joint Marketing	A formal agreement between non-affiliated financial companies that together market financial products or services to you.

Other Important Information

Information for California Customers: You have the right to control whether we share some of your personal information. You have the following rights to restrict the sharing of personal and financial information with our affiliates and outside companies that we do business with. Unless you say “no”, we may share personal and financial information about you with our affiliated companies and with outside companies we may contract with to provide financial products and services to you.