ONLINE PRIVACY AND SECURITY

Widespread use of modern technology carries certain risks and dangers. While Benjamin F. Edwards & Co. ("BFE") and Benjamin F. Edwards Wealth Management, LLC (EWM) take special measures to ensure the safety of your personal information, your efforts can help to maintain your financial security. This Online Privacy and Security notice informs you of the information we collect from you online, and steps you can take to project yourself from internet fraud.

INFORMATION WE COLLECT FROM YOU ONLINE

When you visit our website at www.benjaminfedwards.com, our web servers will collect the name of the domain you used to access the Internet, as well as your computer's Internet Protocol (IP) address. We also may collect information about your device identifier the pages of our website that you visit, the time and date of your visit, the time spent on those pages, the website you came from and visit next, and other diagnostic data. We may collect this information through the use of cookies. We use this information to evaluate the performance of our website and to audit it for security purposes.

Our website also offers several ways in which you can voluntarily provide personally identifiable information to us. For instance, we collect information from you when you submit it to us through our "Contact Us" or "An Invitation from CEO Tad Edwards" web forms. This information includes your name and e-mail address, and may also include your company name, telephone number, city, state, and information that you provide to us in your message. Please do not send us your account number via e-mail.

WHAT ARE COOKIES?

Cookies are files with a small amount of data which may include an anonymous unique identifier. Cookies are sent to your browser from a website and stored on your device. You can instruct your browser to refuse all cookies or to indicate when a cookie is being sent. If you set your browser to not accept cookies, you will limit the functionality we can provide you when you visit our web site.

Our website uses the following types of cookies:

- Strictly Necessary Cookies. These are cookies that are required for the operation of our websites and for you to be able to complete services you request. They include, for example, cookies that enable you to log into secure areas of our website.
- Session Cookies. Session cookies, also known as "temporary cookies," help our website recognize you and the information you provide as you navigate through our website. Session cookies retain information about your activities only for as

long as you remain on our website. Once the web browser is closed, the cookies are deleted.

- Persistent cookies: These cookies remain in operation even after the web browser has closed. For example, they can remember login details and passwords so you don't need to re-enter them every time you visit our website.
- Analytical Cookies. Our websites use Google Analytics to help us evaluate the performance of our website and to give us information about how online visitors use and interact with our website. Google Analytics uses cookies to collect online identifiers, cookie identifiers, IP addresses and device identifiers. To learn more about how Google uses information from sites or apps that use its service, please see Google's Privacy Policy, which is accessible here: https://policies.google.com/privacy.

DO WE SHARE THE INFORMATION WE COLLECT FROM YOU ONLINE?

Yes. It is necessary for us to share this information with third parties for our business purposes and for other reasons as permitted by law. The categories of third persons with whom we share your information are:

- Our affiliates (BFE and EWM);
- Service providers with whom we have contracts to maintain and service our client relationships; market our products and services; manage our client relationships; analyze activity on our website; maintain the security, confidentiality and integrity of our systems and detect fraud;
- Financial institutions with whom we have joint marketing agreements; and
- With other third parties as required and permitted by law.

CAN YOU CORRECT THE INFORMATION THAT WE GATHER ONLINE?

Yes, if you entered information through our "Contact Us" or "An Invitation from CEO Tad Edwards" forms and later need to correct that information, please contact your financial advisor. If you are not a current client, please contact us by calling (855) 382-1600, or by sending your name and contact information to us at privacy@benjaminfedwards.com. Please do not send us your account number via e-mail. Please note that if we cannot associate the information to you, we may not be able to correct it.

DO WE RESPOND TO "DO NOT TRACK" SIGNALS?

No.

CAN OTHER PARTIES COLLECT PERSONALLY IDENTIFIABLE INFORMATION ABOUT YOU WHEN YOU VISIT OUR WEBSITE?

Yes. Our website includes Social Plugins ("buttons") for Facebook, Twitter, YouTube, and LinkedIn. These buttons work by using code from the social media companies that allows you to connect to them from our website, and allows them to collect information about your activity while you are on our website, including your Internet Protocol address, the pages you visit, the

device and browser you are using, and more. You can review the privacy policies of these social media companies to learn more about the data they collect, and how to manage or control the collection of data in your account settings. The privacy policies of these social media companies are available at:

Facebook: https://www.facebook.com/policy.php

Twitter: https://twitter.com/en/privacy

YouTube: https://www.youtube.com/about/policies/#community-guidelines

LinkedIn: https://www.linkedin.com/legal/privacy-policy

WHAT IF YOU LINK TO OTHER WEBSITES FROM OUR WEBSITE?

Our website contains links to websites that are controlled by third parties and provide access to third-party information and services. For example, from our website you may link to FINRA's "Broker Check" page (to check the background of our firm), to "NetXInvestor" (to get instant access to your account and tax statements, trade confirmations and more), to ADP Workforce Now (to apply for employment with us), or to Google, Facebook, Twitter, YouTube and LinkedIn (to view their privacy policies). These links are provided to you as a convenience, and we are not responsible for the content, action or performance of any linked website. Please be aware that other websites have their own privacy policies, and their data gathering practices may be different from ours. We are not responsible for the information collected by other websites if you link to them from our website. We cannot guarantee how those sites use cookies or whether they place cookies on your computer that may identify you. You should carefully review the privacy policies of each website you visit to understand how it collects and uses information.

WHAT IF OUR PRIVACY AND SECURITY NOTICE CHANGES?

We may update this Online Privacy and Security Notice from time to time. We will notify you of any material changes by posting the new Online Privacy and Security Notice on this page, along with the effective date of any changes.

PROTECTING YOURSELF FROM INTERNET FRAUD.

PHISHING

Phishing is the practice of impersonating a trusted company or person in an attempt to gain sensitive information such as Social Security numbers, as well as account numbers and passwords. It is typically conducted by e-mail, but it can also take place over the phone or by mail. Never provide sensitive information to anyone unless you personally know them and there is a valid reason for conveying the information.

Fraudulent e-mails often have the appearance of legitimate messages from financial institutions and retailers. Persons sending these messages are able to alter the "from" address, and add links leading to internet sites similar to trusted sites, when in fact they may host potentially dangerous viruses. These sites will commonly invite you to submit account or credit card information in order to gain information or products and services. It is always safest to type a website's address into your browser rather than to rely on a link contained in an e-mail.

To ensure the safety of your information, follow these guidelines:

- Never enter a password on the Internet unless you know the site to be authentic. Never give your password to anyone electronically or verbally. We will never ask for your password.
- Use antivirus and firewall software and keep them up to date.
- Do not supply credit card or other sensitive information to persons calling by phone. If you wish to obtain products or services from the caller, ask for the company name and their contact information. Verify the information through the phone directory or Internet before calling back.
- If an e-mail appears to be from a trusted institution but contains multiple spelling or grammatical errors, it may in fact be fraudulent.
- If you have reason to suspect that an e-mail message isn't legitimate, do not respond to it. Instead, contact the company that purportedly sent the message to confirm the message's legitimacy.
- Never open unsolicited or unexpected e-mail attachments unless you know the sender and verify that the sender intended to send them.
- Do not store personal information on public or shared computers, and always remember to delete your browsing history before logging out of a shared computer.

IDENTITY THEFT

In addition to immediate financial risk, successful phishing exploits will often expose you to identity theft. Once your sensitive information has been gained by fraudulent individuals, it may be sold to others, used to obtain credit in your name, and may even jeopardize your personal safety.

Your information can also be endangered by burglary, virus intrusions, and "dumpster diving." It is wise to invest in a cross-cut shredder to destroy personal documents, expired credit cards, and unsolicited credit offers. If you use your computer to store or access sensitive information, or to make purchases online, it is essential that you keep your virus protection software current.

If you believe you may be a victim of identity theft you should contact the following credit bureaus to place an alert in your credit records:

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

In addition, you should file a police report and contact the Federal Trade Commission (FTC). You should also contact your financial institutions if you believe your account information may have been compromised.

Effective date: July 2021.