INTEGRITY

INTEGRITY FINANCIAL CORPORATION
PRIVACY POLICY STATEMENT

FACTS	WHAT DOES INTEGRITY FINANCIAL CORPORATION ("INTEGRITY") 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. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect, and share depend on the products or services you have with us. This information can include: – Social Security number, date of birth, and government-issued identification – Income, assets, investment experience, and financial goals – Account balances, transaction history, and portfolio holdings – Contact information, including name, address, email, and telephone number – Employment information and tax identification numbers – Information collected through your use of our website or client portal (e.g., IP address, device identifiers, browsing activity)
How?	All financial companies need to share clients' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their clients' personal information, the reasons Integrity chooses to share, and whether you can limit this sharing.

Reasons we can share your information	Does Integrity share?	Can you limit this sharing?
For our everyday business purposes – such as to 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	We do not share
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	We do not share
For our affiliates to market to you	No	We do not share
For non-affiliates to market to you	No	We do not share

To limit our Sharing	Call (800) 794-4015, or email Dr. Kristofer Gray, Chief Compliance Officer at kgray@ifclegacy.com. *Please note: If you are a new client, we can begin sharing your information thirty (30) days from the date we sent this notice. When you are no longer our client, we continue to share your information as described in this notice. However, you can contact us at any time to limit our sharing.*

INTEGRITY

What we do	
How does Integrity protect my personal information?	To protect your personal information from unauthorized access and use, we maintain comprehensive written information security policies and procedures that include administrative, technical, and physical safeguards designed to: – **Ensure the security and confidentiality** of customer records and information; – **Protect against anticipated threats or hazards** to the security or integrity of customer records and information; and – **Protect against unauthorized access to or use** of customer records and information that could result in substantial harm or inconvenience to any customer. These safeguards include but are not limited to encryption of sensitive data in transit and at rest, multi-factor authentication, access controls, firewalls, intrusion detection systems, employee training programs, and periodic risk assessments. We regularly test and monitor the effectiveness of these safeguards.
How does Integrity collect my personal information?	We collect your personal information, for example, when you: – Open an account or enter into an investment advisory agreement – Provide your income, assets, or investment objectives – Make deposits or withdrawals from your account – Direct us to buy or sell securities or other investments – Communicate with us via phone, email, our website, or client portal – We also collect your personal information from other sources, 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 nonaffiliates 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.
What happens when I limit sharing for an account with multiple beneficial owners?	Your choices will apply to everyone on your account — unless you tell us otherwise.

Service Providers and Third Parties	We may disclose your non-public personal information to non-affiliated third parties as permitted or required by law, including to: – Broker-dealers and custodians that hold your accounts – Service providers who assist us in administering and servicing your accounts (*e.g.*, portfolio accounting, compliance, technology providers). – Financial planning service providers and technology platforms – Regulatory authorities, law enforcement, or as otherwise required by law We require all service providers that have access to your personal information to maintain appropriate safeguards and to limit their use of your information to the purposes for which it was disclosed.

Use of Artificial Intelligence Technology	
Use of Technology and Automation	We use technology tools, including software that may incorporate artificial intelligence or machine-learning capabilities, to support administrative functions, research, compliance monitoring, and client service.
Data Handling and Training	Client personal information is not used to train public artificial intelligence models or shared for such purposes.
Third-Party Vendors	When we engage third-party service providers that utilize artificial intelligence, we require contractual commitments regarding confidentiality, data security, and limitations on the use of client information.
Human Oversight	All advisory services and decisions remain subject to human review and oversight.

Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and non-financial companies. – *Integrity is affiliated with Living Well Family Office and Fintent.*
Non-affiliates	Companies not related by common ownership or control. They can be financial and non-financial companies. *Integrity may share personal information with non-affiliated third parties, such as broker dealers, banks and investment advisers for business purposes. Integrity may also share personal information with parties who provide technical support, legal counsel, and accounting and compliance professionals.*
Joint marketing	A formal agreement between non-affiliated financial companies that together market financial products or services to you. – *Integrity does not have non-affiliated joint marketing partners.*

Incident Response and Data Breach Notification	
Integrity has adopted and implemented written policies and procedures for an Incident Response Program that is reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information, including incidents involving customer information maintained by service providers on our behalf.	
Notification of Data Breaches	In the event that we become aware of an incident involving unauthorized access to or use of your sensitive customer information that has occurred or is reasonably likely to have occurred, and where such incident creates a reasonably likely risk of substantial harm or inconvenience to you, we will notify you as follows: **Timing:** We will provide notice as soon as practicable, but ***no later than thirty (30) days*** after we become aware that the incident has occurred or is reasonably likely to have occurred, unless a federal law enforcement agency determines and communicates to us that notification should be delayed because it would impede a criminal investigation or cause damage to national security. In such cases, notice will be provided promptly after the law enforcement agency determines that notification will no longer pose such a risk. **Content of Notice:** The notification will include, to the extent known at the time: – The incident in general terms; – The type(s) of sensitive customer information that was or is reasonably believed to have been accessed or used without authorization; – Contact information for the Firm, including how you can reach us with questions or concerns; – Contact information for the Federal Trade Commission and, where applicable, information about how to place a fraud alert or security freeze on your credit file; – Recommended steps you should take to protect yourself from potential harm resulting from the incident; and – If applicable, information about any protective services (such as credit monitoring or identity theft protection) we are offering to impacted individuals. **Method of Notice:** We will provide notification by a means designed to ensure that each affected individual can reasonably be expected to receive it, such as direct notification via U.S. mail, email, or telephone. **Notification to Regulatory Authorities:** Subject to the nature and scope of the cybersecurity breach, we will be required to notify regulatory authorities as required by applicable law, including the U.S. Securities and Exchange Commission.
Definition of Sensitive Customer Information	For purposes of this policy, "sensitive customer information" means any component of customer information alone or in conjunction with any other information, the compromise of which could create a reasonably likely risk of substantial harm or inconvenience to an individual identified with the information. This information includes, but is not limited to a customer's name, Social Security number, financial

	account numbers, driver's license number, passport number, and login credentials.

Transfer and Disposal of Customer Information	We have policies and procedures governing the secure transfer and disposal of customer information. When customer information is no longer necessary for business or legal purposes, we ensure it is securely disposed of in a manner consistent with our information security program.

Former Clients	If you decide to close your account(s) or become an inactive client, we will adhere to the privacy policies and practices described in this notice.

For California Residents	In addition to the rights described above, the California Financial Information Privacy Act ("CalFIPA") provides California residents with enhanced protections regarding the sharing of personal financial information. Under CalFIPA: – We will not share your non-public personal information with non-affiliated third parties, other than as permitted by law, unless we first provide you with a clear and conspicuous notice and a reasonable opportunity to opt out of such sharing. – We will not share your non-public personal information with affiliated companies for marketing purposes unless we first provide you with notice and a reasonable opportunity to opt out. – You have the right to opt out of the sharing of your personal financial information with both affiliates (for marketing purposes) and non-affiliated third parties beyond what is permitted under federal law. **To exercise your CalFIPA opt-out rights,** please contact us using the information provided above.

For Washington Residents	Washington residents may have additional privacy rights under applicable Washington state law. To the extent personal information we collect is subject to Washington consumer privacy protections beyond that provided by federal financial privacy law: – **Right to Access.** You have the right to confirm whether we are processing your personal data and to access that data. – **Right to Correct.** You have the right to request that we correct inaccuracies in your personal data. – **Right to Delete.** You have the right to request that we delete personal data you have provided us or that we have obtained about you, subject to permitted exceptions. – **Right to Data Portability.** Where technically feasible, you may request a copy of your personal data in a portable, readily usable format. – **Right to Opt Out.** You have the right to opt out of the processing of your personal data for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects. **Integrity does not sell personal data or engage in targeted advertising or automated profiling that produces legal or similarly significant effects.** – **Right to Appeal.** If we decline to act on your request, you may appeal our decision by contacting us using the information below. We will respond to your appeal within the timeframe required by applicable law.

Updates to this Notice	We reserve the right to change this privacy policy at any time. If we make material changes, we will notify you in accordance with applicable law. We will provide you with a revised privacy notice at least once annually, as required.

Questions or Concerns	If you have any questions about this privacy notice or our privacy practices, please contact us at: **Integrity Financial Corporation** Attn: Chief Compliance Officer 24955 Pacific Coast Highway, Suite B202 Malibu, CA 90265 or email: Dr. Kristofer Gray at kgray@ifclegacy.com

This Privacy Policy Notice is provided in accordance with Regulation S-P (17 CFR Part 248), as adopted and amended by the U.S. Securities and Exchange Commission, including the amendments adopted on May 16, 2024 (SEC Release No. 34-100155), the Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801-6809), and applicable state law.

Dated: 02/17/2026
rev.02/26