plan$well

Eric Arnold, CEO
Planswell USA Corp.
1065 SW 8th Street
Miami, FL 33130

August 4, 2021

Re: Compliance Considerations

After speaking with several compliance departments at major firms, we decided to approach the SEC about the potential need to register as an RIA. We submitted an application and subsequently had a call with three of their lawyers.

The SEC shared multiple reasons why we would not need to register, highlights being:

1) We do not endorse any advisor. We are not paid to promote the advisor to the client. Advisors on our platform have the opportunity to market to our users, much like how a trade show vendor has the ability to contact attendees. Planswell users are attracted to our ecosystem to learn from our calculators and free content. Not because we are promoting advisors.

2) Our plans do not mention securities. Clients use our software to better understand asset allocation optimization across registered accounts, not across asset classes.

3) Advisors do not pay us for clients. They pay for unlimited use of our remote planning software, training, and for the opportunity to market to Planswell users via telephone and email. If a Planswell user decides to become a client of an advisor, there is no change in cost to the advisor and they do so without Planswell suggesting or endorsing any transactions. The advisor is not even required to inform Planswell when they onboard a new client.

After speaking with the SEC, our conclusions were re-affirmed that we do not need to register as an RIA. We welcome any questions or concerns that an advisor or compliance department may have and would appreciate the opportunity to discuss them.

Please see our original commentary, below, followed by an FAQ section:

To Whom It May Concern:

The purpose of this letter is to examine the operational processes of Planswell USA Corp. in the context of regulatory statutes as set forth by the Securities Exchange Commission (SEC) and Financial Industry Regulatory Authority (FINRA). The primary focus of the Planswell business model is to offer free financial plans to visitors of the website, https://planswell.com/

(consumers). In order to provide this service, Planswell provides an online platform for consumers to answer a series of questions about their personal circumstances, which are then entered into proprietary financial planning software and processed through a series of assumptions that are leveraged to build the plan. Once the plan has been created, the consumer is provided with the opportunity to speak with a financial advisor to assist with implementation of the financial plan. Planswell attempts to connect financial professionals with consumers through the financial planning process.

I'll address three primary areas of regulatory focus relevant to the aforementioned financial planning process: advertising compliance, client privacy, and solicitation & referral agreements. These areas of regulatory focus are addressed in both SEC and FINRA regulatory statutes.

Advertising Compliance

SEC Rule 206(4)-1 addresses regulatory guidelines for advertisements by investment advisers (the "SEC Advertising Rule"). Under the rule, an investment adviser is prohibited from publishing, circulating, or distributing any advertisements that:

- Refer to testimonials concerning the adviser or any advice or service of the adviser;
- Refer to past specific recommendations of the adviser which were or would have been profitable to a person (except advertisements that list all recommendations by the adviser for at least one year together with certain required information and required cautionary legend);
- Represent that any graphs, charts, or formula or device can, in and of themselves, be used to determine which securities to buy or sell, or when to buy or sell them unless accompanied by explicit disclosure regarding limitations and serious difficulties and risks inherent with their use;
- Represent that a service will be provided free of charge unless there is in fact no condition or obligation; or
- Contain any "untrue statement of a material fact" or that is "otherwise false or misleading."

Planswell is not required to register as an investment adviser based on the definition of investment adviser in the *Investment Advisers Act of 1940 Section 202(a)(11)*. Additionally, Planswell does not participate in conduct that can be viewed as a violation of the above listed regulatory statutes. Once the registered investment adviser executes an advisory contract with a Planswell consumer, the adviser will be required to properly review and archive all marketing and advertising materials in accordance with the firm's written supervisory procedures. Furthermore, since the RIA is not promoting or administrating the Planswell website, the information contained within the Planswell website does not fall under the supervision of the RIA, and is not required to be archived.

FINRA Rule 2210 addresses communications with the public for FINRA member firms. Planswell is not required to register with FINRA. However, Planswell recognizes that

communications to consumers as a result of utilizing Planswell services will most often fall under the definition of either retail communications or correspondence. Registered principals of broker dealers should therefore review the communications of registered representatives accordingly.

Client Privacy

Planswell understands the importance of maintaining client privacy and confidentiality. The software refrains from requesting client account information, social security numbers, driver's license or passport identification numbers, dates of birth, or any other information that could potentially be misused or mishandled resulting in harm to the consumer. Planswell maintains a detailed and extensive privacy policy, visible at https://planswell.com/privacy-policy.

Regulation S-P requires registered broker dealers, investment companies, and investment advisers to "adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information." When a written advisory contract is executed between the advisor and a Planswell consumer, the adviser will then provide the client with a copy of the firm's Form ADV Part 2 and Privacy Policy. At that point, the RIA will operate according to the firm's written supervisory procedures and corresponding regulatory requirements.

Solicitation and Referral Arrangements

SEC Rule 206(4)-3 is the *Cash Solicitation Rule*. Our interpretation of the rule concludes that the use of Planswell's services do not constitute a solicitation or referral arrangement due primarily to the following factors:

- The payment from the adviser to Planswell is not contingent upon the consumer becoming a client.
- The amount of the ongoing payment does not change after the consumer becomes a client.
- The software is designed to facilitate only financial planning services, and does not in any way foster investment management relationships.
- Planswell users are randomly distributed to advisors in their geographic area, therefore the relationship with Planswell does not constitute an introduction of a specific client from one person or entity to another.
- The ongoing payment from the advisor to Planswell is in exchange for continued access to the software platform, and is not a recurring payment associated with any particular consumer.

Please see our compliance FAQs below for additional commentary on Regulatory Compliance guidance, as well as our Privacy Policy and our attached Data Security Summary. Lastly, I will refer you to our Terms of Service for further information.

Sincerely,

Eric Arnold
CEO
Planswell US Corp.

Compliance Q&A (FAQs)

Q: Is content FINRA reviewed, and does Planswell provide FINRA review letters?
A: No. Planswell's content is not required to be reviewed by FINRA, or any other regulatory agency. Planswell is not a broker dealer, custodian, or an RIA. FINRA letters are only available to FINRA Members, (Broker/Dealers and Custodians).

Q: What tools or processes do you have to ensure that firm compliance officers have the ability to review and approve content before it is disseminated to the public?
A: Planswell's financial planning platform does not send any post plan creation content to clients, and therefore nothing sent by Planswell is considered marketing content being disseminated on behalf of any Broker Dealer or an RIA. As a result, there is no requirement for pre-approval of Planswell's marketing materials.

Q: How are changes to existing content handled to ensure they are approved by compliance prior to going public.
A: Planswell's platform is not configured to allow the advisor to "send" content to a client from Planswell's system. Updates to financial plans do not contain recommendations, or the ability to customize messages sent to clients. There is no original content, or changes to existing content, that will require compliance approval. Planswell is not a broker dealer, custodian, or an RIA.

Q: Are Advisers or Firms able to send anything directly by email or text message through your company's platform?
A: No. Planswell's system is not configured to allow advisers to utilize the system to contact clients. Planswell does not communicate with clients after the original plan is built. In addition, once the lead is assigned to an adviser, Planswell does not communicate with them any further, with the exception of required disclosures for terms of use, privacy policy, and password resets.

Q: Will prospects be loaded into Planswell's CRM in addition to ours? If/when the prospect becomes a client, will that information still be retained with Planswell?
A: Yes, we have the users basic information on our system so they can maintain access to their plan that was created at Planswell. We will retain all information unless there is a request to be removed and then we would honor that request as per our privacy policy. By design, we minimize the amount of data that is retained in general. We only

have the user's first name (no last name) zip, phone and email. We refrain from gathering further detailed PII data.

Q: Who delivers the plans from the client perspective, Planswell or the end advisor?
A: The plan is delivered by Planswell through the self service digital offering online. This plan contains no product or securities recommendations, and operates primarily as an automated tool presenting best practices when it comes to generalized financial planning concepts.

Q: How are the leads distributed?
A: The users are distributed to a single advisor; we do not distribute these users to anyone else. We prioritize distributing users to advisors that are geographically close to the users so there is potential for meeting face to face at some point. We also work to achieve standards when it comes to AUM and Income of the users. Users must meet minimum quality levels to be distributed. For all of these reasons, we have language in our Terms of Service that gives us the power to distribute as we see fit.

Q: What is the quoted fee and payment structure (flat fee, per lead, etc.)?
A:The pricing packages can all be seen on this page here: https://planswell.com/rocket. The fees are monthly with minimum numbers of users to be distributed on a monthly basis and the fees are for access to the entire marketing platform. The price is not tied to the specific users, it is tied to access to the software, our platform, and then the introductions to users on a monthly basis.

Q: Is Planswell registered as a Registered Investment Adviser?
A: No. Planswell is not required to register as an investment adviser based on the definition of investment adviser in the Investment Advisers Act of 1940 Section 202(a)(11).

Q. Is the use of Planswell's services compliant with SEC regulations regarding advertising?
A: Yes. Planswell does not participate in conduct that can be viewed as a violation of SEC Rule 206(4)-1.

Q: How does Planswell view the platform in the context of SEC Rule 206(4)-3, the solicitation and referral arrangement rule?
A: The advisors are not paying for referrals. Advisers are paying for an entire marketing and software platform that also includes client introductions. The ongoing payment from the advisor to Planswell is in exchange for continued access to the software platform, and is not a recurring payment associated with any particular consumer.

Q: Is there a charge to the customer to build financial plans?
A: No. Planswell does not charge consumers. The financial plans are built for free.

Q: How is content disseminated?
A: Planswell does not disseminate content on behalf of the firm.

Q: Are there any additional costs to the adviser for compliance tools?
A: Planswell does not offer compliance services, and therefore does not charge advisers for compliance services. Once the lead becomes a client, the firm will implement their Written Supervisory Procedures as is standard with any other client relationship.

Q: How does Planswell address the privacy rights of the users?
A: Planswell understands the importance of maintaining client privacy and confidentiality. The software refrains from requesting client account information, social security numbers, driver's license or passport identification numbers, dates of birth, or any other information that could potentially be misused or mishandled resulting in harm to the consumer. Planswell maintains a detailed and extensive privacy policy, visible at https://planswell.com/privacy-policy.

Q. How are disclosures utilized on content? Do you use the Financial Professional's specific Broker Dealer/RIA disclosure or in the case of lead generation are you indicating a "Financial Professional" may contact you if you respond?
A: Due to the nature of our business and us not being registered as an RIA, Planswell maintains a privacy policy that details how a user's information will be managed on the platform and that someone may reach out to discuss plan implementation.

Q: In the case of lead generation explain what steps are taken to ensure the prospect understands they will be contacted by a Financial Services Professional and what options they have to opt out
A: Planswell maintains a detailed Privacy Policy which outlines in plain language how the users information will be managed and how users will be referred to one of our partners that will facilitate implementation of their plan. All users have the ability to opt out of any communications and have the right to be deleted as well on our platform. All details can be found here: https://planswell.com/privacy-policy.

Security Outline

DATA CENTERS

Planswell's physical infrastructure is hosted and managed within Amazon's secure data centers and utilize the Amazon Web Service (AWS) technology. Amazon manages risk and undergoes recurring assessments to ensure compliance with industry standards. Amazon's data center have been accredited under (See more details here: AWS Cloud Compliance)

- ISO 27001, ISO 27017, ISO 27018
- SOC 1/SSAE 16/ISAE 3402, SOC 2, SOC 3
- PCI DSS Level 1
- FISMA Moderate
- Sarbanes-Oxley (SOX)
- SEC Rule 17a-4(f)

PHYSICAL SECURITY

Planswell Corp infrastructure utilizes ISO 27001 and FISMA certified data centers managed by Amazon. Amazon has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS platform and infrastructure. AWS data centers are housed in nondescript facilities, and critical facilities have extensive setback and military grade perimeter control berms as well as other natural boundary protection. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, state of the art intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication no fewer than three times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

Amazon only provides data center access and information to employees who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical and electronic access to data centers by Amazon employees is logged and audited routinely.

For additional information see: AWS Cloud Security.

PCI

We use PCI compliant payment processor Stripe for encrypting and processing credit card payments. We do not store any of this information ourselves and rely on Stripe to manage all sensitive payment information. For more details about this, please review Stripe's security documentation: https://stripe.com/docs/security/stripe

Data Center Network Security

FIREWALLS

Firewalls are utilized to restrict access to systems from external networks and between systems internally. By default all access is denied and only explicitly allowed ports and protocols are allowed based on business need. Each system is assigned to a firewall security group based on the system's function. Security groups restrict access to only the ports and protocols required for a system's specific function to mitigate risk.

Host-based firewalls restrict customer applications from establishing localhost connections over the loopback network interface to further isolate customer applications. Host-based firewalls also provide the ability to further limit inbound and outbound connections as needed.

DDOS MITIGATION

Our infrastructure provides DDoS mitigation techniques including connection rate limiting in addition to maintaining multiple backbone connections and internal bandwidth capacity that exceeds the Internet carrier supplied bandwidth. We work closely with our providers to quickly respond to events and enable advanced DDoS mitigation controls when needed.

Data Security

DATA IN TRANSIT

All data transmission between your computer and our servers is encrypted, using the industry-standard HTTPS protocol. We use HTTP Strict Transport Security (HSTS) to ensure only secure connections can be used for our website. Our website is supported by Google Chrome, Edge, and Firefox for this purpose.

DATA AT REST

All your personally identifiable information — including your name, email, and uploaded documents — is encrypted when we store it.

System Security

SYSTEM CONFIGURATION

System configuration and consistency is maintained through standard, up-to-date images, configuration management software, and by replacing systems with updated deployments. Systems are deployed using up-to-date images that are updated with configuration changes and security updates before deployment. Once deployed, existing systems are decommissioned and replaced with up-to-date systems.

SYSTEM AUTHENTICATION

Operating system access is limited to Planswell Corp staff and requires username and key authentication. Operating systems do not allow password authentication to prevent password brute force attacks, theft, and sharing.

New systems are deployed with the latest updates, security fixes, and Planswell configurations and existing systems are decommissioned. This process allows Planswell to keep the environment up-to-date.

VULNERABILITY SCANNING

Planswell Corp employs 3rd parties to support vulnerability scanning and detection of our application. This process is core to our development and operational framework as we assess/ and address any identified vulnerabilities as they present themselves.

VULNERABILITY REPORTING

Planswell Corp takes security very seriously, and investigates all reported vulnerabilities. If you would like to report a vulnerability or have a security concern regarding Planswell Corp services, please email security@planswell.com.

Please provide full details of the suspected vulnerability so the Planswell security team may validate and reproduce the issue.

SOFTWARE SECURITY AND THREAT MANAGEMENT

Planswell leverages industry-grade protocols in the continuous development and delivery of its software products. Threat management and vulnerability testing are performed on a routine basis by our third-party partners with findings (if any) reviewed and resolved promptly.

BACKUPS

All of your data is backed up daily. Planswell Corp maintains at least 7 days of backup data at any given time. In addition, we continuously take snapshots of the database.

ACCESS TO CUSTOMER DATA

Planswell staff does not access or interact with customer data as part of normal operations. There may be cases where Planswell is requested to interact with customer data at the request of the customer for support purposes or where required by law. Planswell may also inspect customer data to debug and troubleshoot platform issues. All of our detailed privacy management policies can be found in our privacy policy: https://planswell.com/privacy-policy/

CONTACT US

If you have any questions about this, please email: hello@planswell.com