UNITED PLANNERS
FINANCIAL SERVICES

DATA PRIVACY & PROTECTION

WHAT WE DO TO PROTECT CONFIDENTIAL CLIENT INFORMATION

7333 E. DOUBLETREE RANCH ROAD
SUITE 120
SCOTTSDALE, AZ 85258
PHONE: 800-966-8737

Member: FINRA, SIPC

Data privacy and protection has become a daily headline with everything from the latest data breaches at major institutions such as Equifax, to intentional exploitation of consumer information by Facebook. Truly understanding how a company protects your confidential information can be difficult as most companies provide standard language privacy and data protection notice that is designed to meet regulatory requirements more than educate clients about what a company does to protect their confidential information. At United Planners Financial Services, we believe that it is important to take the extra step to identify **what we do to protect your confidential client information.**

1 SECURE AUTHENTICATED COMPUTERS AND MOBILE DEVICES

Desktop and laptop computers, tablets and mobile phones are vulnerable to attacks if not adequately protected with required complex passwords, malware/spyware, encryption and other sophisticated security measures. Using a device for email only also creates a cybersecurity risk, as email is one of the most common ways that hackers use to access confidential client information through schemes such as phishing, ransomware, keystroke logging and other illegal and unethical tactics.

United Planners requires all associates use only secure, authenticated devices to conduct business. Every computer and mobile device used to conduct business (including email) is monitored 24/7 with a rigorous check of the device as it connects to United Planners' systems and networks. This includes the strength and age of passwords used, whether the device's critical software is up to date and how the device is accessing United Planners' systems and networks, to include a secure Wi-Fi or approved connection type. We receive notifications when a device is not safe which allows us to fix the problem or deny access to United Planners' systems and networks.

2 SECURE SYSTEMS & NETWORKS AND ONGOING CYBERSECURITY RISK ASSESSMENT

Strong technical and administrative controls to secure internal systems and networks are core to the protection of confidential client information. Most firms employ a variety of basic technical and administrative controls that restrict access to only those individuals who need the access to perform their job. A detailed Cybersecurity Risk Assessment tailored to the company's business model is required to efficiently set up the technical and administrative controls. It also requires implementation of controls and management of the systems and networks by qualified internal staff or a professional Managed Security Service Provider (MSSP). Equally important is oversight or "auditing" of the ongoing security functions performed by external MSSPs or internal staff to ensure that the technical and administrative controls are in place and are properly working.

United Planners completes ongoing Cybersecurity Risk Assessments and has enhanced its technical and administrative controls to address the key risks identified with its internal systems and networks. United Planners uses a professional MSSP to implement and manage its technical and administrative controls, which are continually evaluated to ensure industry requirements and best practices are followed. The MSSP is "audited" by an external third party which verifies that its technical and administrative controls are in place and working properly.

Securing internal systems and networks is critical, but the reality is that confidential client information is also sent, received, accessed and shared across many external networks through the internet to facilitate business. Clients demand easy access to their financial information using the internet. The security risks of data aggregation (i.e. accumulated data from multiple sources or

---

1 — FINRA Investor Alert, Know Before You Share: Be Mindful of Data Aggregation Risks, March 29, 2018

2 — Consumer Financial Protection Bureau, Consumer-authorized financial data sharing and aggregation; Stakeholder insights that inform the Consumer Protection Principals, October 18, 2017

3 — SIFMA, Industry-wide Data Aggregation Principals, April 12, 2018.

accounts shared with authorized users) are well documented by the Financial Industry Regulatory Authority (FINRA)[1], the Consumer Financial Protection Bureau (CFPB)[2], and the Securities Industry and Financial Markets Association (SIFMA)[3]. Most companies rely on a secure Application Programming Interface (API), Virtual Private Network (VPN), encryption or other types of secure connections to send, receive, access or share confidential client information with other companies. Those solutions are slow and unsafe because they are based on a broken security model and do not address the key security problem: the open internet.

United Planners is the first Broker/Dealer (B/D) and Registered Investment Adviser (RIA) to get "Under the Dome,"™ which is secure and off the open internet. The Dome, offered by cleverDome, Inc., provides a global standard of trust where authenticated firms use a secure private network to send, receive, share and access confidential client information. Data is routed off of the open internet and into a private network to access the Dome. Under the Dome, data is fractionalized, or split up into many pieces, and dispersed over multiple channels. The result is a private network that is safe, reliable and 10 times faster than a traditional VPN.

3 THIRD PARTY VENDOR DUE DILIGENCE

Third party vendors have become an essential part of providing software as service and other support to the financial services industry, but these vendors lack regulation and minimum cybersecurity standards to protect confidential client information. B/Ds and RIAs are responsible for ensuring third party vendors they use are adequately protecting confidential client information. This is a massive undertaking that financial services firms struggle with because it requires significant resources and expertise to properly evaluate cybersecurity protections in place at third party vendors.

United Planners utilizes the third party vendor due diligence completed by cleverDome on all cleverDome Members. This means that any software or services vendor, custodian, B/D or RIA who sends, receives, shares or accesses confidential client information successfully completes the cleverDome due diligence process and satisfies minimum cybersecurity standards that meet and/or exceed requirements and guidelines applicable to financial services firms. It also establishes the global standard of trust under the Dome™ because all cleverDome Members are known to each other and have satisfied the due diligence requirements before they send, receive, share or access confidential client information.

4 CYBERSECURITY AWARENESS TRAINING AND TESTING

Utilizing secure devices, systems and networks are crucial components of a strong cybersecurity program, but technology tools alone are not enough. Effective cybersecurity requires a human element. Approximately two-thirds of cybersecurity claims reported to insurers were due to human error, i.e. employees falling prey to phishing links or failing to take preventative measures such as regularly changing passwords.[4] Rigorous training and testing of all individuals involved in servicing financial advisors and their clients reduces the instances of human error that increases cybersecurity risks.

United Planners requires all associates to complete training and testing to identify their vulnerabilities and strengthen their reaction to potentially dangerous situations such as phishing attacks. The training is designed to address common types of attacks targeted at individuals working in the financial services industry, and provide specific guidance based on how the individual reacted to the test.

---

4 — Willis Towers Watson, Decoding Cyber Risk: Driving a Cyber-Savvy Workforce, 2017.

5 INCIDENT RESPONSE PLAN AND CYBERSECURITY INSURANCE

No cybersecurity program is perfect. Human error, nefarious hackers and the need for ever evolving technical controls will eventually lead to a data security breach that results in unintended exposure of confidential client information for some firms. When a breach does occur, the most important step is to respond appropriately. This requires a detailed incident response plan executed by a dedicated team of internal and external resources. Many firms do not have the internal expertise or resources to address data security breaches, which is why cybersecurity insurance is necessary. A comprehensive cybersecurity insurance policy provides not only the financial resources to respond to a data security breach, but also the technical and legal expertise to ensure that the breach is thoroughly investigated and remediated, and that all regulatory requirements are satisfied to include appropriate notifications to clients. Not all B/D or RIA cybersecurity insurance policies provide coverage for independent contractor financial advisors and their businesses, so it is important to understand who and what is covered.

United Planners has implemented and tested its Incident Response Plan. It has dedicated internal resources who are involved in investigating and responding to data security incidents. United Planners also has a comprehensive cybersecurity insurance policy that covers not only United Planners and its home office employees, but also its independent contractor financial advisors and their businesses.

In summary, United Planners has taken several additional steps to secure your client personal information and assist your financial advisor in being cybersecurity compliant beyond the standards set by the industry today. This overview articulates United Planners' commitment to safeguarding confidential client information by establishing strong systems and internal controls that are verified by independent parties. This culture of compliance sets high standards of conduct to build trust with us and to provide you comfort in doing business with United Planners.

United Planners Standard Privacy Policy can be found at:

https://bit.ly/2JEXRsi

for download.

7333 E. DOUBLETREE RANCH ROAD
SUITE 120
SCOTTSDALE, AZ 85258
PHONE: 800-966-8737