BOUSTEAD SECURITIES, LLC WSP SECTIONS 21-24

Cybersecurity 21.0

21.01 Definitions

A. Information Resources (IR): any and all computer printouts, online display devices, magnetic or optical storage media, and all computer-related activities involving any device capable of receiving email, browsing websites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, smart phones, pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e., embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

B. Information Security Officer (ISO): Responsible to the executive management for administering the information security function within the Firm. The ISO is the Firm's internal and external point of contact for all information security matters. The ISO is currently the CTO.

C. Security Administrator: The person charged with monitoring and implementing security controls and procedures for a system. Whereas each The Firm will have one Information Security Officer, technical management may designate a number of security administrators. The Security Administrator is the CTO.

D. System Administrator: Person responsible for the effective operation and maintenance of Information Resources, including implementation of standard procedures and controls to enforce an organization's security policy. The System Administrator is the CTO and CCO.

E. Information Resources Manager (IRM): Responsible to the Firm for the management of the Firm's information resources. The designation of a Firm information resources manager is intended to establish clear accountability for setting policy for information resources management activities. If the Firm does not designate an IRM, the title defaults to the Firm's CEO, and the CEO is responsible for adhering to the duties and requirements of an IRM.

F. Computer Incident Response Team (CIRT): Personnel responsible for coordinating the response to computer security incidents in an organization.

G. User: An individual or automated application or process that is authorized access to the resource by the owner, in accordance with the owner's procedures and rules.

21.02 Disciplinary Actions

A. Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers. Additionally, individuals are subject to loss of Information Resources access privileges, civil, and criminal prosecution.

21.03 Acceptable Use

A. Users must report any weaknesses in the Firm's computer security, any incidents of possible misuse or violation of this agreement to the proper authorities by contacting the appropriate

management.

B. Users must not attempt to access any data or programs contained on The Firm systems for which they do not have authorization or explicit consent.

C. Users must not share their Firm account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes.

D. Users must not make unauthorized copies of copyrighted software.

E. Users must not use any software without the Firm's Information Resources management's approval.

F. Users must not purposely engage in activity that may: harass, threaten or abuse others; degrade the performance of Information Resources; deprive an authorized Firm user access to a Firm resource; obtain extra resources beyond those allocated; or, circumvent Firm computer security measures.

G. Users must not download, install or run security programs or utilities that reveal or exploit weaknesses in the security of a system. For example, the Firm users must not run password cracking programs, packet sniffers, or port scanners or any other non-approved programs on the Firm's Information Resources. The Firm's Information Resources must not be used for personal benefit.

H. Users must not intentionally access, create, store or transmit material which the Firm may deem to be offensive, indecent or obscene (other than in the course of academic research where this aspect of the research has the explicit approval of the Firm's official processes for dealing with academic ethical issues).

I. Access to the Internet from a Firm owned, home based, computer must adhere to all the same policies that apply to use from within the Firm facilities. Employees must not allow family members or other non-employees to access the Firm's computer systems.

J. Users must not otherwise engage in acts against the aims and purposes of the Firm as specified in its governing documents or in rules, regulations and procedures adopted from time to time.

21.04 Incidental Use

A. Incidental personal use of email, internet access, fax machines, printers, copiers, and so on, is restricted to Firm approved users; it does not extend to family members or other acquaintances.

B. Incidental use must not result in direct costs to the Firm.

C. Incidental use must not interfere with the normal performance of an employee's work duties.

D. No files or documents may be sent or received that may cause legal action against, or embarrassment to, the Firm.

E. Storage of personal email messages, voice messages, files and documents within the Firm's Information Resources must be nominal.

F. All messages, files and documents – including personal messages, files and documents – located on Firm Information Resources are owned by the Firm, may be subject to open records requests, and may be accessed in accordance with this policy.

21.05 Account Management

A. All accounts created must have an associated request and approval that is appropriate for the Firm system or service.

B. All users must attest to being provided a copy of the Firm's policies and procedures prior to being given account access.

C. All user accounts must have a unique identifier.

D. All passwords for accounts must be constructed in accordance with the Firm's Password Policy.

E. All accounts must have a password expiration that complies with the Firm's Password Policy.

F. Accounts of individuals on extended leave (more than 30 days) will be disabled.

G. All new user accounts that have not been accessed within 30 days of creation will be disabled.

H. System Administrators or other designated staff (who may or may not be a principal):

1. Are responsible for creating accounts;
2. Are responsible for removing the accounts of individuals that change roles within the Firm or are separated from their relationship with the Firm;
3. Must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes;
4. Must have a documented process for periodically reviewing existing accounts for validity;
5. Are subject to independent audit review;
6. Must provide a list of accounts for the systems they administer when requested by authorized Firm management; and
7. Must cooperate with authorized Firm management investigating security incidents.

21.06 Change Management

A. Security patches on all systems must be implemented within the specified timeframe of notification from the Firm.

B. Every change to an Information Resources resource such as: operating systems, computing hardware, networks, and applications is subject to the Firm's policies.

C. A formal written change request must be submitted to the ISO for all changes, both scheduled and unscheduled.

D. The ISO may deny a scheduled or unscheduled change for reasons including, but not limited to, inadequate planning, inadequate back-out plans, the timing of the change will negatively impact a key business process such as year-end accounting, or if adequate resources cannot be readily available. Adequate resources may be a problem on weekends, holidays, or during special events.

E. Vendor notification must be completed for each scheduled or unscheduled change.

F. A change review must be completed for each change, whether scheduled or unscheduled, and

whether successful or not.

G. A Change Management Log must be maintained for all changes. The log must contain, but is not limited to:

1. Date of submission and date of change;
2. Owner contact information;
3. Nature of the change; or
4. Indication of success or failure.

H. All information systems must comply with an Information Resources change management process that meets the standards outlined above.

21.07 Data Backup

A. The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the data owner.

B. There must be multiple backups of critical information, preferably with different media, vendors and designated personnel (who may or may not be a principal) within each node responsible for backing up data. The persons responsible for backing up data should be independent and not have access to the other's backups.

C. The Firm's Information Resources backup and recovery process for each system must be documented and periodically reviewed.

D. Physical access controls implemented at offsite backup storage locations must meet or exceed the physical access controls of the source systems.

E. A process must be implemented to verify the success of the Firm's electronic information backup.

F. Backups must be periodically tested to ensure that they are recoverable.

G. Employees approved for access to the Firm's backup media held by the offsite backup storage vendor(s) must be reviewed annually or when an authorized individual leaves the Firm.

21.08 Data Destruction

A. All client or company data maintained electronically must be completely erased or destroyed prior to selling, transferring, and/or disposing of any electronic media containing such information. Such electronic media may include, but is not limited to: computers, laptops, tablets, smartphones, photocopiers, fax machines, and USB drives.

B. All Firm owned devices identified for disposal must be given to the ISO.

21.09 Data Encryption

A. Encryption Strength

1. All encryption mechanisms implemented to comply with this policy must support a minimum of, but not limited to the industry standard, AES 128-bit encryption.

2. The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by the Firm.

3. The Firm's key length requirements will be reviewed annually and upgraded as technology allows.

B. Data at Rest

1. Note: hard drives that are not fully encrypted, e.g., have encrypted partitions, virtual disks, or are unencrypted, but connect to encrypted USB devices, may be vulnerable to information spillage from the encrypted region into the unencrypted region. The hard drive's unencrypted auto- recovery folder may retain files that have been saved to the encrypted portion of the disk or USB. Full disk encryption avoids this problem.

2. Confidential data at rest on computer systems owned by and located within the Firm controlled spaces and networks should be protected by at least one of the following:

    a. Encryption;
    b. Firewalls with strict access controls that authenticate the identity of those individuals accessing the systems/data;
    c. Sanitizing the data requiring protection during storage to prevent unauthorized exposure (e.g., truncating last four digits of a Primary Account Number); or
    d. Other compensating controls including: (e.g., complex passwords, physical isolation/access);
    e. Password protection should be used in combination with all controls including encryption. Password protection alone is not an acceptable alternative to protecting confidential information;
    f. The Firm secures its back up and stored data on file systems, disks, heterogeneous tape drives, virtual tape libraries in a Storage Area Network/ Direct-Attached Storage/ Network-Attached Storage environment; or
    g. Confidential back up data is protected using at least AES 128-bit algorithm or identical live data encryption methodologies.

C. Portable Devices

1. Portable devices represent a specific category of devices that contain data- at-rest. Many incidents involving unauthorized exposure of confidential data may be the result of stolen or lost portable computing devices.
2. Each designated Information Resource owner (who may or may not be a principal) will identify information that is confidential.
3. Confidential information stored on portable devices must use Firm approved software.
4. Portable devices including laptops, tablets, and smartphones that store or transmit confidential information must have the proper protection mechanisms installed, including antivirus or firewall software, with unneeded services and ports turned off and subject to needed applications being properly configured.
5. Removable media including CD-ROMs, floppy disks, backup tapes, and USB memory drives that contain confidential information must be encrypted and stored in a secure, locked location.
6. Removable media including CD-ROMs, floppy disks, backup tapes, USB memory drives, etc. that contain confidential information must be transported in a secure manner.
7. Portable or removable media that contain confidential data must be in the possession of the authorized user at all times (e.g., must not be checked as luggage while in transit).
8. The Firm may inventory encrypted devices and validate implementation of encryption products.
9. Data owners and users of portable computing devices and non-Firm owned computing devices

containing confidential data must certify encrypted data will be accessible only by the owner using Firm approved software. The Firm can use any of the methods below in cases where access to confidential information is lost or forgotten:

a. Maintaining an accessible copy of the data on a server managed by the Firm, using procedures specified by the Firm.
b. Use of whole-disk encryption technologies that provide an authorized systems administrator access to the data in the event of a forgotten key.
c. Escrowing the encryption key with a trusted party designated by the data owner and the Information Security Officer.

D. Transmission Security

1. Users will follow acceptable use policies when transmitting data and must take particular care when transmitting or re-transmitting confidential data.
2. Confidential information transmitted as an email message must be encrypted.
3. Any confidential information transmitted through a public network (e.g., Internet) to and from vendors, customers, or entities doing business with the Firm must be encrypted or be transmitted through an encrypted tunnel that is encrypted with virtual private networks (VPN) or end-to-end encryption protocols such as secure sockets layer.
4. Transmitting unencrypted confidential information through the use of web email programs is not allowed.
5. The download or installation of any Instant Messaging (IM) or online peer- to-peer (P2P) file sharing programs requires specific authorization in writing from the Information Resources Manager (IRM) or designated official (who may or may not be a principal). All approved P2P or IM networks will use tools that encrypt the traffic flows between peers and only allow access to a managed IM server which provides gateways to public services.
6. Wireless (Wi-Fi) transmissions that are used to access the Firm's portable computing devices or internal networks must be encrypted using IEEE 802.11i (WPA2) or better.
7. Encryption is required when users access data remotely from a shared network, including connections from a Bluetooth device to a PDA or cell phone.
8. The Firm permits the secure encrypted transfer of documents and data over the Internet using file transfer programs such as "secured FTP" (FTP over SSH) and SCP. Only authorized users can initiate secure FTP or SCP transactions and will use the following procedures:

    a. To use the transmitting server securely, each authorized user must have a logon ID and password with a designated directory. Users should not have access to shared directories unless required for business reasons. Anonymous FTP is not permitted.
    b. All accounts and keys must be managed from within the network.
    c. All transactions and transfers must be logged and reviewed for prohibited activity.
    d. Plain FTP does not provide encrypted transmission and should not be used on any Internet-facing systems or where confidential data is being transmitted.

E. Encryption Key Management

1. Effective key management is the crucial element for ensuring the security of any encryption system. Key management procedures must ensure that authorized users can access and decrypt all encrypted data using controls that meet operational needs and comply with data retention requirements. Key management systems are characterized by the following security precautions:

    - The Firm uses procedural controls to enforce the concepts of least privilege and separation of duties for personnel (per NIST SP800-53 guidelines). These controls apply to persons involved in encryption key management or who have access to security-relevant encryption key facilities and processes, including Certificate Authority (CA) and Registration Authority (RA), and/or contractor personnel. The ISO will verify backup storage for key passwords, files, and related backup configuration

data to ensure access to encrypted data.

a. The ISO conducts regular audit trail reviews.
b. The ISO or designated individuals (who may or may not be a principal) who do not authorize the issuing certificates will verify the subject's identity.
c. Background checks and clearance procedures are required for the personnel who have access to encryption keys.
d. Any personnel that has access to encryption keys must complete regular training on key management requirements and procedures.
e. Sanctions may be used against personnel for unauthorized actions, unauthorized use of authority, and unauthorized use of The Firm systems, include written reprimand or dismissal.
f. The Firm will collect a written acknowledgement of receipt of this policy from each individual involved in key management.

2. Key management should be fully automated, so personnel do not have the opportunity to expose a key or influence the key creation.
3. Keys in storage and transit must be encrypted.
4. Private keys must be kept confidential and stored in a secure manner.
5. Keys must be randomly chosen from the entire key space, using hardware- based randomization.
6. Key-encrypting keys are separate from data keys. No data ever appears in clear text that was encrypted using a key-encrypting key, e.g., a key- encrypting-key is used to encrypt other keys, securing them from disclosure.
7. Keys that are transmitted are sent securely to well-authenticated parties.
8. Key-generating equipment is physically and logically secure from construction through receipt, installation, operation, and removal from service.
9. The key management system or vendor will provide written security policies and procedures that address encryption key:
    a. Generation processes for different cryptographic systems and different applications;
    b. Distribution, access, and activation for authorized users;
    c. Storage, archiving, and destruction;
    d. Changes and updates, including rules on when keys should be changed and how this will be done;
    e. Compromises or loss of control incidents;
    f. Revocation with specific withdrawal or deactivation procedures;
    g. Recovery when lost or corrupted as part of business continuity planning;
    h. Roles, responsibilities, facilities, and procedures for all organizational elements to reliably recover critical data;
    i. Specification of circumstances and process for authorizing key recovery;
    j. Storage and access for long-term storage keys;
    k. Process of transitioning from the current to future long-term storage keys;
    l. Audit logging of management-related activities; and
    m. Activation and deactivation dates and usage period limits.

F. Exceptions
1. The Information Resource owner should be the person responsible for establishing data encryption policies that might include granting exceptions based upon demonstration of a business need and an assessment of the risk of unauthorized access to or loss of the data.
2. Under certain circumstances the ISO may grant or issue an exception to the use of encryption on portable computing devices and non-Firm owned computing devices containing confidential data.
3. Exceptions are of two types:
    a. An exception may be granted to address the specific circumstances or business needs relating to an individual program or department. Requests for exceptions of this type should be in writing and should be initiated by the data owner.

b. Broader exceptions may be issued to cover circumstances that span the Firm as a whole. Requests for exceptions of this type may come from any person, or such exceptions may be initiated by the ISO.

4. The ISO, CCO and/or data owner must approve and document all exceptions based on an assessment of business requirements weighed against the likelihood of an unauthorized exposure and the potential adverse consequences for individuals, other organizations, or the Firm if an exposure occurs as a result of the exception.
5. As a condition for granting an exception, the ISO may require implementation of compensating controls to offset the risk created by the lack of encryption.
6. Exceptions must be documented and must include the following elements:
    a. A statement defining the nature and scope of the exception in terms of the data included and/or the class of devices included;
    b. The rationale for granting the exception;
    c. An expiration date for the exception; and
    d. A description of any compensating security measures that are to be required.

21.10 Business or Firm Electronic Mail

A. The following activities are prohibited by policy:
1. Sending business email that is intimidating or harassing.
2. Using business email for purposes of political lobbying or campaigning.
3. Violating copyright laws by inappropriately distributing protected works.
4. Posing as anyone other than oneself when sending business email, except when authorized to send messages for another when serving in an administrative support role.
5. The use of unauthorized Firm email software.

B. The following activities are prohibited because they impede the functioning of network communications and the efficient operations of Firm email systems:
1. Sending or forwarding chain letters.
2. Sending unsolicited messages to large groups except as required to conduct the Firm business.
3. Sending or forwarding business email that is likely to contain computer viruses.
4. All sensitive Firm material transmitted over external network must be encrypted.
5. All user activity on the Firm's Information Resources assets is subject to logging and review.
6. Firm email users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the Firm or any unit of the Firm unless appropriately authorized (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer will be included unless it is clear from the context that the author is not representing the Firm. An example of a simple disclaimer is: "the opinions expressed are my own, and not necessarily those of my employer."
7. Individuals must not send, forward or receive confidential or sensitive Firm information through non-Firm email accounts. Examples of non-Firm email accounts include, but are not limited to, Gmail, Yahoo mail, AOL mail, and email provided by other Internet Service Providers (ISP).
8. Individuals must not send, forward, receive or store confidential or sensitive Firm information utilizing non-Firm approved mobile devices. Examples of mobile devices include, but are not limited to, two- way pagers and cellular telephones.

21.11 Incident Management

A. The Firm CIRT members have pre-defined roles and responsibilities which can take priority over normal duties.

B. Whenever a security incident, such as a virus, worm, hoax email, discovery of hacking tools, altered data, etc. is suspected or confirmed, the appropriate Incident Management procedures must be followed.

C. The ISO is responsible for notifying the IRM and the CIRT and initiating the appropriate incident management action including restoration as defined in the Incident Management Procedures.

D. The ISO is responsible for determining the physical and electronic evidence to be gathered as part of the Incident Investigation.

E. The appropriate technical resources from the CIRT are responsible for monitoring that any damage from a security incident is repaired or mitigated and that the vulnerability is eliminated or minimized where possible.

F. The ISO, working with the IRM, will determine if a widespread The Firm communication is required, the content of the communication, and how best to distribute the communication.

G. The appropriate technical resources from the CIRT are responsible for communicating any new issues or vulnerabilities to the system vendor and working with the vendor to eliminate or mitigate the vulnerability.

H. The ISO is responsible for initiating, completing, and documenting the incident investigation with assistance from the CIRT.

I. The ISO is responsible for:

1. Reporting the incident to the IRM;
2. Reporting the incident to the local, state or federal law officials as required by applicable statutes and/or regulations; and
3. Coordinating communications with outside organizations and law enforcement, as needed.

J. In the case where law enforcement is not involved, the ISO will recommend disciplinary actions, if appropriate, to the IRM.

K. In the case where law enforcement is involved, the ISO will act as the liaison between law enforcement and the Firm.

21.12 Internet Use

A. Software for browsing the Internet on Firm owned devices is provided to authorized users for business and research use only.

B. All software used to access the Internet on Firm owned devices must be part of the Firm standard software suite or approved by the ISO. This software must incorporate all vendor provided security patches.

C. All files downloaded from the Internet on Firm owned devices must be scanned for viruses using the approved IS distributed software suite and current virus detection software.

D. All software used to access the Internet on Firm owned devices shall be configured to use the firewall.

E. All sites accessed on Firm owned devices must comply with Firm Acceptable Use Policies.

F. All user activity on Firm owned devices Information Resources assets is subject to logging and review.

G. Content on all Firm websites must comply with the Firm's Acceptable Use Policies.

H. No offensive or harassing material may be made available via Firm websites.

I. Non-business related purchases made over the Internet on Firm owned devices are prohibited. Business related purchases are subject to Firm procurement rules.

J. No personal commercial advertising may be made available via Firm websites.

K. The Firm's Internet access on Firm websites or Firm owned devices may not be used for personal gain or non-Firm personal solicitations.

L. No Firm data will be made available via Firm websites without ensuring that the material is available to only authorized individuals or groups.

M. All sensitive Firm material transmitted over external networks must be encrypted.

N. Electronic files are subject to the same records retention rules that apply to other documents and must be retained in accordance with departmental records retention schedules.

O. Incidental Use

1. Incidental personal use of Internet access on Firm owned devices is restricted to Firm approved users; it does not extend to family members or other acquaintances.
2. Incidental use on Firm owned devices must not result in direct costs to the Firm. Incidental use on Firm owned devices must not interfere with the normal performance of an employee's work duties.
3. No files or documents may be sent or received that may cause legal liability for, or embarrassment to, the Firm.
4. Storage of personal files and documents within the Firm's Information Resources should be nominal.
5. All Firm related files and documents – including personal files and documents on Firm owned devices – are owned by the Firm, may be subject to open records requests, and may be accessed in accordance with this policy.

21.13 Mobile Computing

A. Only Firm approved portable computing devices may be used to access Firm Information Resources.

B. Employees granted permission to use their own personal portable computing device must sign the Firm acceptable use policy that includes the requirement that the employee surrender their device at the request of the Firm for any investigation.

C. Firm owned portable computing devices may not be "cracked," "rooted" or "jailbroken;" and users may not use any other means to bypass the security features of any Firm owned mobile device or Firm software.

D. Firm owned portable computing devices and Firm software must be kept patched and updated.

E. Employees may not install unsigned applications on any Firm owned portable computing

device.

F. Firm owned portable computing devices and Firm software must be password protected using the strongest password controls available on the device.

G. Firm owned portable computing devices and Firm software will make use of two-factor authentication whenever possible.

H. Firm owned portable computing devices and Firm software must run current anti-virus and anti-malware software and those applications must be kept current.

I. Firm owned portable computing devices and Firm software will be centrally managed.

J. The Firm data may not be stored on any non-Firm portable computing devices or non-Firm software. However, in the event that there is no alternative to local storage, all sensitive Firm data must be encrypted using approved encryption techniques. The storage of sensitive or confidential data on a portable computing device must be approved by the CTO, CCO and data owner.

K. All remote access to the Firm data must be through a secure connection.

L. Non-Firm computer systems that require network connectivity to access Firm data must conform to Firm Standards and must be approved in writing by the ISO.

M. Firm owned portable computing devices or Firm software should not be left unattended even for brief periods of time. Such devices should not be left in cars or packed in checked luggage.

N. Lost or stolen Firm owned portable computing devices or non-Firm portable devices that have Firm software or Firm data on it must be reported to the ISO.

O. Firm owned portable devices and Firm enabled software for business email will have remote wiping enabled or remote wiping applications, as applicable, installed as a protection if such device is lost, stolen or if personnel is separated or terminated from the Firm.

P. All Firm owned portable computing devices must be surrendered to the ISO and Firm business email is terminated upon separation of the employee from the Firm.

Q. The ISO will maintain an inventory of all Firm owned portable computing devices that contain Firm or client data or that have access to Firm systems as well as a list of who has access to Firm software such as business email.

21.14 Network Access

A. Users are permitted to use only those network addresses issued to them by the Firm on Firm owned devices.

B. All remote access on Firm owned devices or to access Firm software will be through an approved connection.

C. Users must not add, extend or re-transmit network services in any way. This means you must not install a router, switch, hub, or wireless access point to the Firm network without the Firm's approval.

D. Non-Firm computer systems that require Firm network connectivity to Firm software must conform to the Firm's Standards. This includes home computers.

E. Users must not download, install or run security programs or utilities that reveal weaknesses in the security of a system on any Firm owned device. For example, Firm users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the Firm's network infrastructure.

F. Users are not permitted to alter Firm network hardware that accesses Firm data in any way.

21.15 Network Configuration

A. The Firm's Information Services owns and is responsible for the Firm's network infrastructure and will continue to manage further developments and enhancements to this infrastructure

B. To provide a consistent Firm network infrastructure capable of exploiting new networking developments, all cabling must be installed by the Firm or an approved contractor.

C. All Firm network connected equipment must be configured to a specification approved by the Firm.

D. All hardware connected to the Firm network is subject to the Firm's management and monitoring standards.

E. Changes to the configuration of active Firm network management devices must not be made without the approval of the Firm.

F. The Firm's network infrastructure supports a well-defined set of approved networking protocols. Any use of non-sanctioned protocols must be approved by the Firm.

G. The networking addresses for the Firm supported protocols are allocated, registered and managed centrally by the Firm.

H. All connections of the Firm network infrastructure to external third-party networks is the responsibility of the Firm. This includes connections to external telephone networks.

I. The Firm's firewalls must be installed and configured following the Firm's standards.

J. The use of Firm departmental firewalls is not permitted without the written authorization from the Firm.

K. Users must not add, extend or re-transmit network services in any way. This means you must not install a router, switch, hub, or wireless access point to the Firm network without the Firm's approval.

L. Users must not install network hardware or software that provides network services without the Firm's approval.

M. Users are not permitted to alter network hardware in any way.

21.16 Password Management

A. All passwords, including initial passwords, must be constructed and implemented to use for Firm business according to the following Firm rules:

    1. It must be routinely changed

2. It must adhere to a minimum length as established by the Firm
3. It must be a combination of alpha, numeric, and special characters
4. It must not be anything that can easily be tied back to the account owner such as: user name, social security number, nickname, relative's names, birth date, etc.
5. Password history must be kept to prevent the reuse of a password.

B. User account passwords for Firm software must not be divulged to anyone.

C. Security tokens (i.e., Smartcard), if applicable, must be returned on demand or upon termination of the relationship with the Firm.

D. If the security of a password to access Firm software or a Firm owned device is in doubt, the password must be changed immediately.

E. Administrators must not circumvent the Password Policy for the sake of ease of use.

F. Firm owned computing devices must not be left unattended for long periods of time without enabling a password protected screensaver or logging off of such device.

G. Help Desk password change procedures must include the following:

1. Authenticate the user to the helpdesk before changing password
2. Change to a strong password
3. The user must change password at first login.
4. In the event Firm software or Firm owned device passwords are found or discovered, the following steps must be taken:

- Take control of the passwords and protect them;
- Report the discovery to the Firm Help Desk;
- Transfer the passwords to an authorized person as directed by the ISO.

H. Password Guidelines for Firm owned devices and to access Firm software:

1. Passwords must be changed when prompted.
2. Passwords must have a minimum length of 8 alphanumeric characters.
3. Passwords must contain a mix of upper and lower case characters and have at least 2 numeric characters. The numeric characters must not be at the beginning or the end of the password. Special characters should be included in the password where the computing system permits. The special characters are (!@#$%^&*_+=?/~`;:,<>|\).
4. Passwords must not be easy to guess and they:
    a. must not be your Username
    b. must not be your employee number
    c. must not be your name
    d. must not be family member names
    e. must not be your nickname
    f. must not be your social security number
    g. must not be your birthday
    h. must not be your license plate number
    i. must not be your pet's name
    j. must not be your address
    k. must not be your phone number
    l. must not be the name of your town or city
    m. must not be the name of your department
    n. must not be street names
    o. must not be makes or models of vehicles
    p. must not be any information about you that is known or is easy to learn (favorite -

food, color, sport, etc.)

q. Passwords must not be reused for a period of one year
r. Passwords must not be shared with anyone
s. Passwords must be treated as confidential information

I. Creating Strong Passwords

1. Combine short, unrelated words with numbers or special characters. For example: eAt42peN
2. Make the password difficult to guess but easy to remember
3. Consider padding passwords by adding a string of repetitive characters to the beginning, middle or end of an otherwise strong password. For example add 0123456789 or $$$$$$$$$$ to pad a password.
4. Substitute numbers or special characters for letters. (But do not just substitute) For example: livefish - is a bad password but L1veF1sh - is better and satisfies the rules, but setting a pattern of 1st letter capitalized, and i's substituted by 1's can be guessed. I!v3f1Sh++++++++++++ - is far better, the capitalization and substitution of characters is not predictable and padding to 20 characters makes this password very strong but still relatively easy to type.

21.17 Physical Security

A. All physical security systems for the Firm must comply with all applicable regulations such as, but not limited to, building codes and fire prevention codes.

B. Physical access to all Information Resources restricted facilities must be documented and managed.

C. All facilities must be physically protected in proportion to the criticality or importance of their function at the Firm.

D. Access to Information Resources facilities must be granted only to the Firm's support personnel, and contractors, whose job responsibilities require access to that facility.

E. The process for granting card and/or key access to Information Resources facilities must include the approval of the person responsible for the facility.

F. Each individual that is granted access rights to an Information Resources facility must receive emergency procedures training for the facility and must sign the appropriate access and non-disclosure agreements.

G. Requests for access must come from the applicable Firm data/system owner.

H. Access cards and/or keys must not be shared or loaned to others.

I. Access cards and/or keys that are no longer required must be returned to the person responsible for the Information Resources facility. Cards must not be reallocated to another individual bypassing the return process.

J. Lost or stolen access cards and/or keys must be reported to the person responsible for the Information Resources facility.

K. Cards and/or keys must not have identifying information other than a return mail address.

L. All facilities that allow access to visitors will track visitor access with a sign in/out log.

M. A service charge may be assessed for access cards and/or keys that are lost, stolen or are not

returned.

N. Card access records and visitor logs for Information Facilities must be kept for routine review based upon the criticality of the Information Resources being protected.

O. The person responsible for the Information Resources facility must remove the card and/or key access rights of individuals that change roles within the Firm or are separated from their relationship with the Firm

P. Visitors must be escorted in card access controlled areas of Information Resources facilities.

Q. The person responsible for the Information Resources facility must review access records and visitor logs for the facility on a periodic basis and investigate any unusual access.

R. The person responsible for the Information Resources facility must review card and/or key access rights for the facility on a periodic basis and remove access for individuals that no longer require access.

21.18 Security Monitoring

A. Automated tools will provide real time notification of detected wrongdoing and vulnerability exploitation. Where possible a security baseline will be developed and the tools will report exceptions. These tools will be deployed to monitor:
    1. Internet traffic
    2. Email traffic
    3. LAN traffic, protocols, and device inventory
    4. Operating system security parameters

B. The following files will be checked for signs of wrongdoing and vulnerability exploitation at a frequency determined by risk:
    1. Automated intrusion detection system logs
    2. Firewall logs
    3. User account logs
    4. Network scanning logs
    5. System error logs
    6. Application logs
    7. Data backup and recovery logs
    8. Help desk trouble tickets
    9. Telephone activity – Call Detail Reports
    10. Network printer and fax logs

C. The following checks will be performed at least annually by assigned individuals:
    1. Unauthorized network devices
    2. Unauthorized personal web servers
    3. Unsecured sharing of devices
    4. Unauthorized modem use
    5. Operating System and Software Licenses

D. Any security issues discovered will be reported to the ISO for follow-up investigation.

21.19 Security Training

A. All users must sign an acknowledgement stating they have read and understand the Firm's requirements regarding computer security policies and procedures.

B. All users (employees, consultants, contractors, temporaries, etc.) must be provided with sufficient training and supporting reference materials to allow them to properly protect the Firm's information resources.

C. The ISO must develop and maintain a communications process to be able to communicate new computer security program information, security bulletin information, and security items of interest.

21.20 Server Hardening

A. A server must not be connected to the Firm's network until a server is hardened and a network connection is approved by the Firm.

B. The Server Hardening Procedure provides the detailed information required to harden a server. Some of the general steps included in the Server Hardening Procedure include:
    1. Installing the operating system from an approved source
    2. Applying vendor supplied patches
    3. Removing or disabling unnecessary software, system services, and drivers
    4. Setting security parameters, file protections and enabling audit logging
    5. Disabling or changing the password of default accounts

C. The Firm will monitor security issues, both internal to the Firm and externally, and will manage the release of security patches on behalf of the Firm.

D. The Firm will test security patches against core resources before release where practical.

E. The Firm may make hardware resources available for testing security patches in the case of special applications.

F. Security patches must be implemented within the specified timeframe of notification from The Firm.

21.21 Vendor Access

A. The Firm will segregate sensitive network resources from resources accessible to third parties.

B. Vendors must comply with all applicable the Firm policies, practice standards and agreements, including, but not limited to, as applicable:
    1. Safety Policies
    2. Privacy Policies
    3. Physical Security Policies
    4. Auditing Policies
    5. Software Licensing Policies

C. Vendors must comply with all applicable the Firm cybersecurity policies, practice standards and agreements, including, but not limited to:
    1. Acceptable Use Policies
    2. Network Access Policies

D. Vendor agreements and contracts must specify:

1. The Firm information the vendor should have access to
2. How the Firm information is to be protected by the vendor
3. Acceptable methods for the return, destruction or disposal of The Firm information in the vendor's possession at the end of the contract
4. The Vendor must only use the Firm's information and Information Resources for the purpose of the business agreement
5. Any other Firm information acquired by the vendor in the course of the contract cannot be used for the vendor's own purposes or divulged to others

E. The Firm will provide a point of contact for the Vendor. The point of contact will work with the Vendor to confirm the Vendor is in compliance with these policies.

F. Each vendor must provide the Firm with a list of all employees working on the contract. The list must be updated and provided to the Firm within 24 hours of staff changes.

G. Each on-site vendor employee must acquire a Firm identification badge that will be displayed at all times while on the Firm's premises. The badge must be returned to the Firm when the employee leaves the contract or at the end of the contract.

H. Each vendor employee with access to the Firm's sensitive information must be cleared to handle that information.

I. Vendor personnel must report all security incidents directly to the appropriate Firm personnel.

J. If vendor management is involved in the Firm's security incident management the responsibilities and details must be specified in the contract.
    1. Vendor must follow all applicable Firm change control processes and procedures.
    2. Regular work hours and duties will be defined in the contract. Work outside of defined parameters must be approved in writing by appropriate Firm management.
    3. All vendor maintenance equipment on the Firm network that connects to the outside world via the network, telephone line, or leased line, and all The Firm IR vendor accounts will remain disabled except when in use for authorized maintenance.
    4. Vendor access must be uniquely identifiable and password management must comply with the Firm's Password Management Policy. Vendor's major work activities must be entered into a log and available to The Firm management upon request. Logs must include, but are not limited to, such events as personnel changes, password changes, project milestones, deliverables, and arrival and departure times.

K. Upon departure of a vendor employee from the contract for any reason, the vendor will ensure that all sensitive information is collected and returned to the Firm or destroyed within 24 hours.

L. Upon termination of contract or at the request of the Firm, the vendor will return or destroy all Firm information and provide written certification of that return or destruction within 24 hours.

M. Upon termination of contract or at the request of the Firm, the vendor must surrender all Firm identification badges, access cards, equipment and supplies immediately. Equipment and/or supplies to be retained by the vendor must be documented by authorized Firm management.

N. All software used by the vendor in providing service to the Firm must be properly inventoried and licensed.

O. The Firm will conduct a review of its vendor's security controls at least on an annual basis. Such review will be conducted by the Firm's CTO with the oversight by the Chief Compliance Officer. Such annual review will be documented in an annual report prepared by the Firm's CTO.

21.22 Virus and Malware Protection

A. All workstations whether connected to the Firm network, or standalone, must use the Firm's IS approved virus protection software and configuration.

B. The virus protection software must not be disabled or bypassed.

C. The settings for the virus protection software must not be altered in a manner that will reduce the effectiveness of the software.

D. The automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates.

E. Each file server attached to the Firm's network must utilize Firm IS approved virus protection software and setup to detect and clean viruses that may infect file shares.

F. Each email gateway must utilize The Firm IS approved email virus protection software and must adhere to the IS rules for the setup and use of this software.

G. Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the CTO.

Regulation Best Interest 22.0

Introduction

Effective as of June 20, 2020 the Securities and Exchange Commission ("Commission") has implemented Regulation Best Interest, which establishes a new standard of conduct under the Securities Exchange Act of 1934 ("Exchange Act") for broker-dealers and their associated person when making a recommendation of any securities transaction or investment strategy involving securities (including account recommendations) to a retail customer.

When making such a recommendation to a retail customer, the firm must act in the best interest of the retail customer at the time the recommendation is made, without placing its financial or other interest ahead of the retail customer's interests.

This general obligation is satisfied only if the firm complies with four specified component obligations:

- Disclosure Obligation: provide certain required disclosure before or at the time of the recommendation, about the recommendation and the relationship between the firm and its retail customer;
- Care Obligation: exercise reasonable diligence, care, and skill in making the recommendation;
- Conflict of Interest Obligation: establish, maintain, and enforce written policies and procedures reasonably designed to address conflicts of interest; and
- Compliance Obligation: establish, maintain, and enforce written policies and procedures reasonably designed to achieve compliance with Regulation Best Interest.

Record-making and Recordkeeping: Additionally, the firm must also comply with new record-making and recordkeeping requirements.

22.01 Recommendations

Regulation Best Interest applies to recommendations of any securities transaction or investment strategy involving securities (including account recommendations) to a retail investor.

Definition of Recommendation

The determination of whether a broker-dealer has made a recommendation that triggers application of Regulation Best Interest turns on the facts and circumstances of a particular situation, and therefore, whether a recommendation has been made is not susceptible to a bright line definition. Factors considered in determining whether a recommendation has taken place include whether the communication "reasonably could be viewed as a 'call to action'" and "reasonably would influence an investor to trade a particular security or group of securities." The more individually tailored the communication to a specific customer or targeted group of customers about a security or group of securities, the greater the likelihood that the communication may be viewed as a "recommendation."

The SEC interprets whether a recommendation has been made to a retail customer that triggers the best interest obligation consistent with precedent under the anti-fraud provisions of the federal securities laws as applied to broker-dealers and with how the term has been applied under the rules of self-regulatory organizations (such as FINRA).

Regulation Best Interest does not apply to investment advice provided to a retail customer by a dual-registrant when acting in the capacity of an investment adviser, even if the retail customer has a brokerage relationship with the dual-registrant or the dual-registrant executes the transaction in a brokerage

capacity.

- ***Account recommendations*** include recommendations of securities account types generally (e.g., to open an IRA or other brokerage account), as well as recommendations to roll over or transfer assets from one type of account to another (e.g., a workplace retirement plan account to an IRA). As discussed more below, special considerations exist where the financial professional making the recommendation is dually registered.
- Any securities transaction or investment strategy involving securities includes:
  - explicit hold recommendations; and
  - implicit hold recommendations that are the result of agreed-upon account monitoring between the broker-dealer and retail customer. Special considerations for providing agreed-upon account monitoring are discussed more below.

Application of Regulation Best Interest for Dually Registrants
If the firm is a financial professional who is dually registered (i.e., an associated person of a broker-dealer and a supervised person of an investment adviser (regardless of whether the firm works for a dual-registrant, affiliated firm, or unaffiliated firm)) making an account recommendation to a retail customer, whether Regulation Best Interest or the Advisers Act applies will depend on the capacity in which the firm is acting when making the recommendation. If the firm is acting as a broker-dealer or associated person thereof, the firm must comply with Regulation Best Interest and will need to take into consideration all types of accounts that the firm offers (i.e., both brokerage and advisory accounts) when making the recommendation of an account that is in the retail customer's best interest.

Application of Regulation Best Interest for BD-Only Registrants
If the firm is only registered as an associated person of a broker-dealer (regardless of whether that broker-dealer entity is a dual-registrant or affiliated with an investment adviser), Regulation Best Interest will apply to that account recommendation, but the firm needs to take into consideration only the brokerage accounts available. The firm can only recommend a brokerage account that the broker-dealer offers if the firm has a reasonable basis to believe that the recommended brokerage account is in the best interest of the retail customer, and the broker-dealer otherwise complies with Regulation Best Interest.

Special considerations for agreed-upon account monitoring
The firm may agree with a retail customer to take on additional obligations beyond those imposed by Regulation Best Interest. For example, the firm may agree with a retail customer to provide monitoring of the firm's retail customer's investments on a periodic basis for purposes of recommending changes in investments.

When the firm agrees with a retail customer to monitor that customer's account: (1) the firm is required to disclose the terms of such account monitoring services (including the scope and frequency of such services) pursuant to the Disclosure Obligation; and (2) such agreed-upon monitoring involves an implicit recommendation to hold (i.e., recommendation not to buy, sell, or exchange assets pursuant to that securities account review) at the time the agreed-upon monitoring occurs.

(a) Scope of monitoring:
Regulation Best Interest does not impose a duty to monitor a retail customer's account. In addition, it does not change the scope of account monitoring that the firm may agree to provide. Regulation Best Interest also does not change the scope of activities that would come within the "solely incidental" prong of the broker-dealer exclusion to the definition of "investment adviser" in the Advisers Act.[3] The firm may choose to adopt policies and procedures that, if followed,

would help demonstrate that any agreed-upon monitoring is in connection with and reasonably related to the firm's primary business of effecting securities transactions.

(b) Agreed-upon monitoring:
If the firm agrees with a retail customer to perform account monitoring services, the firm is taking on an obligation to review and make recommendations with respect to that account (e.g., to buy, sell or hold) on the specified, periodic basis that the firm has agreed to with the retail customer. For example, if the firm agrees to monitor the firm's retail customer's account on a quarterly basis, the quarterly review and each resulting recommendation to purchase, sell, or hold will be a recommendation subject to Regulation Best Interest.

(c) Implicit hold recommendations:
If the firm has agreed to perform account monitoring services, then Regulation Best Interest applies even where the firm remains silent (i.e., an implicit hold recommendation).

(d) Voluntary account review:
The firm may voluntarily, and without any agreement with the firm's customer, review the holdings in the firm's retail customer's account for the purposes of determining whether to provide a recommendation to the customer. This voluntary review is not considered to be "account monitoring," nor would it in itself create an implied agreement with the retail customer to monitor the customer's account.
Any explicit recommendation made to the firm's retail customer as a result of any such voluntary review would be subject to Regulation Best Interest.

22.02 Definition of Retail Customer

A "retail customer" is a natural person, or the legal representative of such person, who:

- receives a recommendation of any securities transaction or investment strategy involving securities from a broker-dealer; and
- uses the recommendation primarily for personal, family, or household purposes.

Legal Representative
A "legal representative" of such person includes the non-professional legal representatives of such a natural person, for example, a non-professional trustee that represents the assets of a natural person.

"Uses" of a Recommendation
We interpret that a retail customer "uses" a recommendation of a securities transaction or investment strategy involving securities when, as a result of the recommendation:

- the retail customer opens a brokerage account with the broker-dealer, regardless of whether the broker-dealer receives compensation;
- the retail customer has an existing account with the broker-dealer and receives a recommendation from the broker-dealer, regardless of whether the broker-dealer receives or will receive compensation, directly or indirectly, as a result of that recommendation; or
- the broker-dealer receives or will receive compensation, directly or indirectly as a result of that recommendation, even if that retail customer does not have an account at the broker-dealer.

Personal, Family, or Household Purposes

A retail customer who uses the recommendation primarily for "personal, family or household purposes" means *any* recommendation to a natural person for his or her account would be subject to Regulation Best Interest, other than recommendations to natural persons seeking these services for commercial or business purposes.

22.03 The Disclosure Obligation

The firm must, prior to or at the time of the recommendation, provide the retail customer, in writing, full and fair disclosure of:

- all material facts relating to the *scope and terms of the relationship with the retail customer*; and
- all material facts relating to *conflicts of interest that are associated with the recommendation*.

Material Facts Requiring Disclosure

- Material facts relating to the scope and terms of the relationship with the retail customer include:
  - that the broker, dealer, or such natural person is acting as a broker, dealer, or an associated person of a broker-dealer with respect to the recommendation;
  - material fees and costs that apply to the retail customer's transactions, holdings, and accounts; and
  - the type and scope of the services to be provided to the retail customer, including any material limitations on the securities or investment strategies that may be recommended to the retail customer.
- Other material facts relating to the type and scope of services provided to the retail customer, and that must be disclosed, include:
  - whether or not the firm will monitor the retail customer's account and the scope and frequency of any account monitoring services that the firm agrees to provide; and
  - whether the firm has any requirements for retail customers to open or maintain an account or establish a relationship, such as a minimum account size.
- Other material facts relating to the scope and terms of the relationship with the retail customer that must be disclosed include:
  - general basis for the firm's recommendations (i.e., what might commonly be described as the firm's investment approach, philosophy, or strategy); and
  - risks associated with the firm's recommendations in standardized terms.
- Additionally, the firm must consider, based on the facts and circumstances, whether there are other material facts relating to the scope and terms of the relationship with the retail customer that need to be disclosed.

Conflict of Interest

For purposes of Regulation Best Interest a "conflict of interest" is defined to mean "an interest that might incline a broker, dealer, or a natural person who is an associated person of a broker or dealer – consciously or unconsciously – to make a recommendation that is not disinterested."

- Such conflicts include, for example: conflicts associated with proprietary products, payments from third parties, and compensation arrangements.
- Broker-dealers must disclose all material facts relating to conflicts of interest associated with the recommendation.

For purposes of Regulation Best Interest, "material facts" is interpreted consistent with the standard articulated in *Basic v. Levinson*. Accordingly, information is material if there is a "substantial likelihood that a reasonable shareholder would consider it important." In the context of Regulation Best Interest, the standard is the retail customer, as defined in the rule.

Full and Fair Disclosure
The Release contains guidance on what constitutes "full and fair" disclosure under Regulation Best Interest. The firm's obligation to provide full and fair disclosure should give sufficient information to enable a retail investor to make an informed decision with regard to the recommendation.

Fees and Costs
The Release contains guidance on what fees and costs must be disclosed. The Disclosure Obligation requires disclosure of material fees and costs relating to a retail customer's transactions, holding, and accounts. This obligation would not require individualized disclosure for each retail customer. Rather, the use of standardized numerical or other non-individualized disclosure (e.g., reasonable dollar or percentage ranges) is permissible.

Fees and costs are material and must be disclosed if there is a "substantial likelihood that a reasonable shareholder would consider it important."

We would generally expect that, to satisfy the Disclosure Obligation, you would build upon the material fees and costs identified in the Form CRS (Relationship Summary), providing additional detail as appropriate.

Time and Substance of Disclosures
Although the disclosures necessary to satisfy the Disclosure Obligation must be in writing, in certain circumstances, the firm may satisfy the firm's Disclosure Obligation by making supplemental oral disclosure not later than the time of the recommendation, provided that you maintain a record of the fact that oral disclosure was provided to the retail customer.

In addition, in the limited instances where existing regulations permit disclosure after the recommendation is made (e.g., trade confirmation, prospectus delivery), the firm may satisfy the firm's Disclosure Obligation regarding the information contained in the applicable disclosure document by providing such document to the firm's retail customer after the recommendation is made.

Oral Disclosures Write these
The Firm will update this section in future revisions.

Disclosure After the Recommendation Write these
The Firm will update this section in future revisions.

Initial written disclosure
Before supplementing, clarifying or updating written disclosures in the limited circumstances described above, the firm must provide an initial disclosure in writing that identifies the material fact and describes the process through which such fact may be supplemented, clarified or updated. For example:

- **Product-level fees:** With regard to product-level fees, the firm could provide an initial standardized disclosure of product-level fees generally (e.g., reasonable dollar or percentage ranges), noting that further specifics for particular products appear in the product prospectus, which will be delivered after a transaction in accordance with the delivery method the retail customer has selected, such as by mail or electronically.
- **Capacity**: Similarly, with regard to the disclosure of a broker-dealer's capacity, a dual-registrant could disclose that recommendations will be made in a broker-dealer capacity unless otherwise expressly stated at the time of the recommendation, and that any such statement will be made orally.
- **Associated Person Conflicts of Interest**: A broker-dealer could disclose that its associated persons may have conflicts of interest beyond than those disclosed by the broker-dealer, and that associated persons will disclose, where appropriate, any additional material conflicts of interest not later than the time of a recommendation, and that any such disclosure will be made orally.

Meeting the Obligation Through the Relationship Summary or Form CRS

Although the firm may use a Relationship Summary and other standardized disclosures about the firm's products and services to help satisfy the Disclosure Obligation, these disclosures may not be sufficient to satisfy the Disclosure Obligation.

Whether the Relationship Summary standing alone, or any additional or existing disclosures, satisfy any of these required disclosures in full would depend on the facts and circumstances.

In most instances, the firm will need to provide additional information beyond that contained in the Relationship Summary in order to satisfy the Disclosure Obligation.

Use of "Adviser" or "Advisor"

The Commission presumes that the use of the terms "adviser" and "advisor" in a name or title by (i) a broker-dealer that is not also registered as an investment adviser or (ii) an associated person that is not also a supervised person of an investment adviser to be a violation of the capacity disclosure requirement under Regulation Best Interest.

22.04 The Care Obligation

Under the Care Obligation, the firm must exercise reasonable diligence, care, and skill when making a recommendation to a retail customer to:

- understand potential risks, rewards, and costs associated with recommendation, and have a reasonable basis to believe that the recommendation could be in the best interest of at least some retail customers**;**
- have a reasonable basis to believe the recommendation is in the best interest of a particular retail customer based on that retail customer's investment profile and the potential risks, rewards, and costs associated with the recommendation and does not place the interest of the broker-dealer ahead of the interest of the retail customer; and
- have a reasonable basis to believe that a series of recommended transactions, even if in the retail customer's best interest when viewed in isolation, is not excessive and is in the retail

customer's best interest when taken together in light of the retail customer's investment profile.

Whether the firm has complied with the Care Obligation will be evaluated as of the time of the recommendation (and not in hindsight).

Components of the Care Obligation

The firm must exercise reasonable diligence, care, and skill to understand the potential risks, rewards, and costs associated with the recommendation.

Reasonable Diligence, Care and Skill

What would constitute reasonable diligence, care, and skill will vary depending on, among other things, the complexity of and risks associated with the recommended security or investment strategy and the broker-dealer's familiarity with the recommended security or investment strategy.

While every inquiry will be specific to the particular broker-dealer and the recommended security or investment strategy, the firm generally should consider important factors such as:

- the security's or investment strategies:
  - investment objectives;
  - characteristics (including any special or unusual features);
  - liquidity;
  - volatility; and
  - likely performance in a variety of market and economic conditions;
- the expected return of the security or investment strategy; and
- any financial incentives to recommend the security or investment strategy.

Together, this inquiry should allow the firm to develop a sufficient understanding of the security or investment strategy and to be able to reasonably believe that it could be in the best interest of at least some retail customers.

Risks Rewards and Costs

The firm must consider the risks, rewards, and costs in light of the retail customer's investment profile and have a reasonable basis to believe that the recommendation is in that particular customer's best interest and does not place the broker-dealer's interest ahead of the customer's interest.

The retail customer's investment profile is defined to include, but is not limited to the retail customer's:

- age;
- other investments;
- financial situation and needs;
- tax status;
- investment objectives;
- investment experience;
- investment time horizon;
- liquidity needs;
- risk tolerance; and
- any other information the retail customer may disclose to the broker in connection with a recommendation

Transactions in a Series

When recommending a series of transactions, the firm must have a reasonable basis to believe that the transactions taken together are not excessive, even if each is in the firm's customer's best interest when viewed in isolation. The requirement applies irrespective of whether the firm exercises actual or *de facto* control over a customer's account.

What would constitute a "series" of recommended transactions would depend on the facts and circumstances and would need to be evaluated with respect to a particular retail customer.

Reasonably Available Alternatives
The firm should consider reasonably available alternatives, if any, offered by the firm in determining whether the firm has a reasonable basis for making the recommendation.

This exercise would require the firm to conduct a review of such reasonably available alternatives that is reasonable under the circumstances, which will depend on the facts and circumstances at the time of the recommendation.

Considerations Specific to IRA Recommendations

- With respect to account type recommendations, the firm should generally consider:
  - the services and products provided in the account;
  - the projected cost to the retail customer of the account;
  - alternative account types available;
  - the services requested by the retail customer; and
  - the retail customer's investment profile.
- When making recommendations to open an IRA, or to roll over assets into an IRA, the firm should consider a variety of factors including, but not limited to:
  - fees and expenses;
  - level of services available;
  - available investment options;
  - ability to take penalty-free withdrawals;
  - application of required minimum distributions;
  - protections from creditors and legal judgments;
  - holdings of employer stock; and
  - any special features of the existing account.

Consideration Specific to Complex or Risky Strategies
When recommending securities or investment strategies that are complex, such as inverse or leveraged exchange-traded products, you should take particular care to make sure you understand the terms, features, and risks – as with the potential risks, rewards, and costs of any security or investment strategy – in order to establish a reasonable basis to recommend the product to retail customers. Further, the firm must weigh the potential risks, rewards, and costs of the particular product or investment strategy, in light of the particular retail customer's investment profile.

Thus, when recommending such products, the firm should understand that inverse and leveraged exchange-traded products that are reset daily may not be in the best interest of retail customers who plan to hold them for longer than one trading session, particularly in volatile markets. Further, these

products may not be in the best interest of a retail customer absent an identified, short-term, customer-specific trading objective.

Similarly, when recommending potentially-high risk products, such as penny stocks or other thinly-traded securities, you should generally apply heightened scrutiny to whether such investments are in the firm's retail customer's best interest.

Considerations Relative to Cost of Recommendations
While The firm must understand and consider costs when making a recommendation, it is only one important factor among many factors. Thus, the firm would not satisfy the Care Obligation by simply recommending the least expensive or least remunerative security without any further analysis of the other factors and the retail customer's investment profile.

For example, depending on the facts and circumstances, the firm may be able to recommend a more expensive security or investment strategy if there are other factors about the product or strategy that reasonably allow the firm to believe it is in the best interest of the firm's retail customer, based on that retail customer's investment profile.

22.05 Conflict of Interest Obligation

The Conflict of Interest Obligation (and the Compliance Obligation discussed below), applies solely to the broker- dealer entity, and not to the associated persons of a broker-dealer.

Under the Conflict of Interest Obligation, a broker-dealer must establish, maintain, and enforce written policies and procedures reasonably designed to address conflicts of interest associated with its recommendations to retail customers.

Specifically, the written policies and procedures must be reasonably designed to:

- Identify and at a minimum disclose, pursuant to the Disclosure Obligation, or eliminate all conflicts of interest associated with such recommendations;
- Identify and mitigate any conflicts of interest associated with such recommendations that create an incentive for the broker-dealer's associated persons to place their interest or the interest of the broker-dealer ahead of the retail customer's interest;
- Identify and disclose any material limitations, such as a limited product menu or offering only proprietary products, placed on the securities or investment strategies involving securities that may be recommended to a retail customer and any conflicts of interest associated with such limitations, and prevent such limitations and associated conflicts of interest from causing the broker-dealer or the associated person to place the interest of the broker-dealer or the associated person ahead of the retail customer's interest; and
- Identify and eliminate sales contests, sales quotas, bonuses, and non-cash compensation that are based on the sale of specific securities or specific types of securities within a limited period of time.

Policies to Mitigate Incentives
The firm's policies and procedures must be reasonably designed to reduce the potential effect such conflicts may have on a recommendation given to a retail customer.

The firm has flexibility to develop and tailor reasonably designed policies and procedures that include conflict mitigation measures, based on the firm's circumstances, such as the firm's size, retail customer base (for example, the diversity of investment experience and financial needs), and the complexity of the security or investment strategy involving securities that is being recommended, some of which may be

weighed more heavily than others.

Policies and procedures may be reasonably designed at the outset, but may later cease to be reasonably designed based on subsequent events or information obtained, for example, through supervision (e.g., exception testing) of associated person recommendations. The firm's actual experience should be used to revise the firm's measures as appropriate.

Specific Mitigation Measures

There are a number of different kinds of incentives and, depending on the specific characteristics of an incentive, different levels and types of mitigation measures may be necessary.

For example, incentives tied to asset accumulation generally would present a different risk and require a different level or kind of mitigation, than variable compensation for similar securities, which in turn may present a different level or kind of risk and may require different mitigation methods than differential or variable compensation or financial incentives tied to broker-dealer revenues.

In certain instances, compliance with existing supervisory requirements and disclosure may be sufficient, for example, where a broker-dealer may develop a surveillance program to monitor sales activity near compensation thresholds.

Potential Mitigation Measures

The following non-exhaustive list of practices could be used as potential mitigation methods for broker-dealers to comply with the mitigation requirement:

- avoiding compensation thresholds that disproportionately increase compensation through incremental increases in sales;
- minimizing compensation incentives for employees to favor one type of account over another; or to favor one type of product over another, proprietary or preferred provider products, or comparable products sold on a principal basis, for example, by establishing differential compensation based on neutral factors;
- eliminating compensation incentives within comparable product lines by, for example, capping the credit that an associated person may receive across mutual funds or other comparable products across providers;
- implementing supervisory procedures to monitor recommendations that are:
    - near compensation thresholds;
    - near thresholds for broker-dealer recognition;
    - involve higher compensating products, proprietary products or transactions in a principal capacity; or,
    - involve the roll over or transfer of assets from one type of account to another (such as recommendations to roll over or transfer assets in an ERISA account to an IRA) or from one product class to another;
- adjusting compensation for associated persons who fail to adequately manage conflicts of interest; and
- limiting the types of retail customer to whom a product, transaction or strategy may be recommended.

Material Limitations on Recommendations

A "material limitation" placed on the securities or investment strategies involving securities that may be recommended would include, for example, recommending only:

- proprietary products, that is, any product that is managed, issued, or sponsored by the financial institution or any of its affiliates;
- a specific asset class;
- or products with third-party arrangements, that is, revenue sharing.

In addition, the fact that the firm recommends only products from a select group of issuers could also be a material limitation.

We recognize that, as a practical matter, almost all broker-dealers limit their offerings of securities and investment strategies to some degree. We do not believe that disclosing the fact that a broker-dealer does not offer the entire possible range of securities and investment strategies would convey useful information to a retail customer, and therefore we would not consider this fact, standing alone, to constitute a material limitation. Rather, consistent with the examples of a "material limitation" provided above, whether the limitation is material will depend on the facts and circumstances of the extent of the limitation.

Mitigation Specific to Material Recommendations

The firm has flexibility to develop and tailor reasonably designed policies and procedures to prevent such limitations and the associated conflicts from causing the broker-dealer or an associated person from placing their interest ahead of the retail customer's interest.

In developing such policies and procedures, the firm should, for example, consider establishing product review processes for products that may be recommended, including establishing procedures for identifying and mitigating the conflicts of interests associated with the product, or declining to recommend a product where the firm cannot effectively mitigate the conflict, and identifying which retail customers would qualify for recommendations from this product menu.

As part of this process, the firm may consider:

- evaluating the use of "preferred lists;"
- restricting the retail customers to whom a product may be sold;
- prescribing minimum knowledge requirements for associated persons who may recommend certain products; and
- conducting periodic product reviews to identify potential conflicts of interest, whether the measures addressing conflicts are working as intended, and to modify the mitigation measures or product selection accordingly.

Conflicts that Require Elimination

The firm must develop written policies and procedures reasonably designed to eliminate sales contests, sales quotas, bonuses and non-cash compensation that are based on the sales of specific securities and specific types of securities within a limited period of time. These practices, when coupled with a time limitation, create high-pressure situations for associated persons to engage in sales conduct contrary to the best interest of retail customers.

This requirement does not apply to compensation practices based on, for example, total products sold, or

asset growth or accumulation, and customer satisfaction.

This elimination requirement would not prevent a broker-dealer from offering only proprietary products, placing material limitations on the menu of products, or incentivizing the sale of such products through its compensation practices, so long as the incentive is not based on the sale of specific securities or types of securities within a limited period of time.

The elimination requirement is not intended to prohibit:

- Training or education meetings, provided that these meetings are not based on the sale of specific securities or types of securities within a limited period of time;
- Receipt of certain employee benefits by statutory employees, as we do not consider these benefits to be non-cash compensation for purposes of Regulation best Interest.

22.06 The Compliance Obligation

The Compliance Obligation, as with the Conflict of Interest Obligation, applies solely to the broker-dealer entity, and not to its associated persons.

The firm must establish, maintain and enforce written policies and procedures reasonably designed to achieve compliance with Regulation Best Interest.

This is an affirmative obligation with respect to the rule as a whole and provides flexibility to allow you to establish compliance policies and procedures that accommodate the firm's business model.

Whether policies and procedures are reasonably designed will depend on the facts and circumstances of a given situation. You should consider, when adopting policies and procedures, the nature of the firm's operations and how to design such policies and procedures to prevent violations from occurring, detect violations that have occurred, and to correct promptly any violations that have occurred.

The firm's compliance policies and procedures should be reasonably designed to address and be proportionate to the scope, size, and risks associated with the firm's operations and the types of business in which you engage.

In addition to the required policies and procedures, depending on the firm's size and complexity, a reasonably designed compliance program generally would also include:

- controls;
- remediation of non-compliance;
- training; and
- periodic review and testing.

22.07 Record-making and Recordkeeping

The firm must meet new record-making and recordkeeping requirements with respect to certain information collected from or provided to retail customers in connection with Regulation Best Interest. This builds upon existing record-making and recordkeeping obligations.

- For each retail customer to whom a recommendation of any securities transaction or investment strategy involving securities is or will be provided, The firm must keep a record of all information

collected from and provided to the retail customer pursuant to Regulation Best Interest, as well as the identity of each natural person who is an associated person, if any, responsible for the account.

- The firm must retain all records of the information collected from or provided to each retail customer for at least six years after the earlier of the date the account was closed or the date on which the information was replaced or updated.

The Firm will be drafting and implementing a summary that stratifies the requirements by June 30, 2020.

Customer Relationship Summary 23.0

On June 5, 2019, the SEC adopted Form CRS and new rules, as well as amendments to its forms and rules, under both the Investment Advisers Act of 1940 ("Advisers Act") and the Securities Exchange Act of 1934. Form CRS and its related rules require SEC-registered investment advisers and SEC-registered broker-dealers (together, "firms") to deliver to retail investors a brief customer or client relationship summary that provides information about the firm. Firms must file their relationship summaries with the SEC.

The relationship summary is designed to assist retail investors with the process of deciding whether to (i) establish an investment advisory or brokerage relationship, (ii) engage a particular firm or financial professional, or (iii) terminate or switch a relationship or specific service. Firms must follow certain requirements concerning their relationship summaries including formatting, filing, delivery, updating, and recordkeeping requirements.

Under rule 17a-14 under the Securities Exchange Act of 1934 and rule 204-5 under the Investment Advisers Act of 1940, broker-dealers registered under section 15 of the Exchange Act and investment advisers registered under section 203 of the Advisers Act are required to deliver to *retail investors* a *relationship summary* disclosing certain information about the firm. Read all the General Instructions as well as the particular item requirements before preparing or updating the *relationship summary*.

If you do not have any *retail investors* to whom you must deliver a *relationship summary*, you are not required to prepare or file one. See also Advisers Act rule 204-5; Exchange Act rule 17a-14(a).

See Form CRS as a separate attachment.

The Firm will be drafting and implementing a summary that stratifies the requirements by June 30, 2020.

Fully Disclosed Clearing Arrangement 24.0

The Firm and Vision Financial Markets, LLC ("Vision") have entered into an agreement whereby the Firm will introduce accounts on a fully disclosed basis to Vision for execution and clearing services.

The Firm has partnered with Vision to provide additional services to underserved markets, issuers, investors, and other financial industry partners.