PEEL HUNT

INFORMATION PROTECTION AND IDENTITY THEFT PREVENTION PROGRAM

July 2025

Contents

1. Introduction

Over the past decade, the incidence of breaches of confidential information and identity theft has grown exponentially. To address these problems, the federal government and most states have adopted rules and regulations to try to protect non-public information and protect the identity of individuals.

While most states only require notification once a breach has been detected, the Commonwealth of Massachusetts has enacted a law that requires firms that do business with Massachusetts residents, and that receive or store non-public information on these residents, to develop procedures to protect this information at all times, to educate their personnel regarding these requirements, and to inform the state of any breaches to their information systems.

Peel Hunt, Inc. (the "Firm") is committed to protecting the non-public information it possesses on its customers, employees and vendors to help mitigate the risk of identity theft without regard to their state of residence.

The Firm only does business with institutional customers and therefore is not subject to the requirements of Reg S-P or S-ID.

However, since information may be gathered relative to employees, registered representatives or other individuals who have an affiliation or interaction with the Firm, the Firm may be subject to requirements under various state rules and is, therefore, adopting procedures to protect such information.

In addition, the Firm is providing information on the requirements under Reg. S-ID as an educational and informational resource to its registered representatives, associated persons and Principals.

2. Regulation S-ID

This policy must be read in conjunction with the Enterprise Risk Management Framework (ERMF). It sets out the minimum requirements that Peel Hunt, as a firm need to comply with, for effective management of Inappropriate Market Conduct and Insider Dealing risks.

2.1. Summary

Reg. S-ID requires financial institutions and creditors, as defined by the 1934 Act, to establish procedures to identify "red flags" during various stages of the relationship with their customers and to take action to mitigate damages that could occur from breaches in their information systems. Reg. S-ID provides the following relevant definitions:

"Financial institution" means a depository or other institution that directly or indirectly holds a transaction account belonging to a consumer.

"Transaction account" means an account that permits the account holder to make withdrawals for payment or transfer to third parties of securities or funds via telephone transfers, check, debit card or similar items.

"Consumer" within these definitions refers only to individuals as customers, not institutions.

"Creditor" means any person who regularly extends, renews, or continues credit or regularly arranges for the extension, renewal or continuation of credit. This would include introducing or clearing firms providing margin, or firms arranging loans, even if for institutional customers.

"Covered accounts" means:

a) an account offered or maintained primarily for personal, family or household purposes that is designed to permit multiple payments or transactions—e.g., "retail" accounts; or

b) any other accounts, including institutional accounts, if they pose a foreseeable risk to the Firm's customers or to its own safety and soundness from identity theft.

2.2. Determination of Applicability of Reg S-ID

Given these definitions and the Firm's business the Chief Compliance Officer ("CCO") has determined that the Firm is neither a "financial institution" nor a "creditor" as defined in Reg. S-ID, and therefore is not required to comply with the Red Flags Rules.

The CCO will periodically reassess this determination if the Firm changes its business operations and will develop and implement a Written Identity Theft Program if deemed required.

2.3. Red Flag Procedures

Identifying misuse or misappropriation of customer information can be difficult and can occur during various stages of the Firm's relationship with a customer.

To assist in identifying possible incidents of misuse of customer information or identity theft, registered representatives and other Firm personnel must be vigilant in reviewing and monitoring account documentation and customer requests.

A key way in which representatives can help identify potential identity theft is through information gathered during the account opening stage and throughout the customer relationship.

The Firm has procedures in place related to knowing customers and verification of identity that can be found in the Firm's Written Supervisory Procedures ("WSP") and Anti-Money Laundering Compliance Program ("AMLCP").

Registered Representatives ("RR(s)") and associated personnel should pay particular attention to the following when opening new accounts or when gathering information from a new customer:

Suspicious documents:

– Documents provided for identification appear to have been altered or forged.

– Information on the new account form is inconsistent with information already received from the customer or on application documents.

– An application appears to have been altered or forged or appears to have been destroyed and reassembled.

RRs or other Firm personnel that suspect possible identity theft or misappropriation of account information should review their suspicions with their supervisor, compliance or another designated Principal so the Firm can determine the validity of the suspicions and take actions to try to determine what steps to take to protect the customer.

Principals in their review of transactions will also watch for potential indications of identity theft or misappropriation of account information.

The CCO will also monitor notices and warnings received from other financial institutions, law enforcement or other third parties relating to potential identity theft or other illegal activities.

The designated Principal will review a list of the Firm's customers, as well as documentation related to potential new customers, to determine if such notices are related to any individuals doing business with, or seeking to do business with, the Firm.

If he or she determines that such an individual has an account with the Firm or is attempting to engage in business with the Firm, he will investigate the circumstances and will notify the appropriate regulatory or law enforcement agency promptly.

2.4. Procedures to Mitigate Risk

The Firm introduces customers and orders to its parent, Peel Hunt LLP for execution, clearing, and settlement.

The Firm does not hold customer accounts, funds or securities directly and relies on its clearing firm to have systems and procedures in place to protect accounts from unauthorized access or misappropriation of customer information.

The CCO will periodically verify that Peel Hunt LLP is monitoring and testing its systems and will seek evidence of such from the Firm's compliance or other applicable areas. Reliance on the parent does not diminish the Firm's responsibility to be vigilant in trying to identify potential "red flags" or for bringing suspected breaches to the attention of the clearing firm, customer and appropriate regulatory or law enforcement agencies as warranted.

The Firm also implements the following procedures to help protect access to accounts or other information:

- Passwords assigned to operations and trading personnel must be changed at least every 90 days and may not be given to any person other than the person to which it was assigned.
- Passwords will be set up to include a combination of numbers, letters and special characters.
- The Firm does not provide Customers with direct access to the Firm's clearing system and so no Customer passwords will be set up by the clearing Firm's system and will not be known to the Firm, its registered representatives or other personnel.
- Accounts and other systems will be locked if someone attempts to login more than five times with an incorrect login identification/password combination. Only the clearing firm can unlock an account for a customer or Firm personnel.

Customers are encouraged to also be vigilant in reviewing their account information and to notify the Firm of any discrepancies as soon as possible.

RRs and other Firm personnel who have access to customer account information will be required to review the Firm's procedures upon hire and will receive training at least annually on any changes to rules, regulations or procedures related to data protection.

The CCO will maintain a record of training in each person's registration or personnel file.

Personnel who have reason to believe that a customer has been the victim of identity theft or that an account has been compromised must immediately bring this information to the attention of the CCO.

FAILURE TO DO SO WILL RESULT IN PROMPT AND DOCUMENTED DISCIPLINARY ACTION AND MAY RESULT IN CRIMINAL OR CIVIL PENALTIES IF THE IDENTITY THEFT OR MISAPPROPRIATION IS PROVEN.

3. Protection of Non-Public Information

Non-public personal information is generally defined as information received from a natural person that includes the person's first and last name or first initial and last name, plus one or more of the following:

- The person's complete social security number;
- A complete financial account or credit/debit card number; or
- A complete government-issued identification number, including but not limited to a driver's license number or passport number.

The Firm gathers non-public information, as defined above on employees or registered representatives, and only gathers that information necessary to conduct its business and provide products and services to its customers and employees.

Only personnel required to have such information in order to fulfil the purpose for which it is gathered shall have access to the information.

The persons designated to review certain areas of the organization, such as the CCO or Head of Human Resources ("HR") r shall review the information gathered by their respective areas of supervision to determine that only information required to fulfil that areas responsibilities is being gathered and that persons not authorized to receive the information do not have access to such.

The Firm has evaluated the types of non-public personal information received and the potential risks regarding the security, confidentiality and integrity of such information.

To comply with various state and federal requirements related to the protection of non-public personal information, the Firm has developed procedures to protect the information at various stages of use within the Firm, to provide training to its personnel relating to the protection of such information and to detect and prevent breaches.

All persons who may have access to non-public information will be trained on Firm policies and regulatory requirements when hired. In addition, the Firm shall provide annual training to any persons with access to such information, persons responsible for the implementation of Firm policies, and Information Technology ("IT") personnel or vendors as deemed necessary based on changes to policies, rules or regulations and the type of information being gathered or retained. The Firm will keep records related to training in the individual's personnel or vendor file.

RRs, operations personnel and all other persons in the Firm with access to non-public personal information gathered by the Firm must be familiar with these procedures and must adhere to them at all times.

Failure to follow Firm procedures as outlined throughout this ITPP or to report potential breaches to the security of non-public personal information shall result in disciplinary action. The types of disciplinary action to be taken will be determined by the applicable Principal or manager based on the facts and circumstances of the situation as well as its severity.

3.1. Information Gathering

Information is gathered from various individuals prior to or at the time they become associated with the Firm.

This information can be gathered in various ways and is used for different purposes, depending on the relationship with the Firm. In all cases, non-public information must be gathered in such a manner as to prevent unauthorized access to the information.

NON-PUBLIC INFORMATION MUST BE MAINTAINED IN A PRIVATE LOCATION AND IN A MANNER DETERMINED BY THE FIRM, SUCH AS NEW ACCOUNT FORMS OR EMPLOYMENT APPLICATIONS.

Information should not be recorded on documents or in a manner not consistent with Firm policies and when Firm personnel take information over the telephone, the information should not be repeated in areas where persons not entitled to the information may overhear the conversation.

3.2. Transmission and Delivery of Information

Firm personnel are responsible for the security of non-public information from the time it is received until it is eventually disposed of by the Firm at the end of the relationship with the customer, employee or vendor.

The process of delivering information to the Firm's files following its receipt is important as failure to deliver information properly can result in the information being compromised or stolen.

The CCO or the Head of HR is responsible for ensuring that the Firm's policies related to the delivery of non-public information are followed and that any misappropriation or loss of such information is immediately reported to:

- The individuals whose information was compromised, and
- Applicable state or federal regulatory or law enforcement agencies.

3.2.1 Paper Document

When information is captured on paper and must be delivered to the Firm from an external location, it is very important that the delivery of this information is secure. Failure to keep control of documents during physical delivery can result in information being obtained by unauthorized persons or being lost.

Personnel charged with delivering information to the Firm's files from external locations must keep it in secure, locked vessels when available or must ensure that information is kept from the sight of others and it is kept in their control at all times.

3.2.2 Telephone Delivery

When information is to be delivered to the Firm by an associated person from an external location via telephone, the individual delivering the information must verify the identity of the person receiving the information by obtaining this person's name and department.

If the telephone is not answered, as is generally required by the Firm, or the person is unknown to the individual providing the information, the individual should not provide the information and should call back to verify that the number dialed was correct. At no time should information be provided to a person unknown to the deliverer.

Prior to providing information, the individual delivering this information must ensure that the area from which he or she is delivering the information is private and information is not overheard by persons who are not authorized to receive it.

Providing non-public information from public areas is strictly prohibited. The recipient of the information must also ensure that no information is repeated if he/she is in a public area or in an area where information may be heard by unauthorized persons.

When providing information to someone over the telephone, the person providing such information must verify the identity of the recipient by asking questions to help identify the person that would not be easily ascertained from identification documents or account information, such as a zip code or the last four digits of their social security number.

Information requested will be predetermined by the Firm and may include a telephone PIN, the name of the person's pet or some other personal identifying information that cannot generally be obtained from documentation or public records.

If the person requesting the information is unable to provide the information requested to identify them, no information may be provided and the designated Principal must be notified immediately.

3.2.3 Electronic Delivery

When information is captured on paper or electronically and is transmitted to the Firm via email or other electronic means, the information must be sent only to email addresses authorized by the Firm to receive such information.

Under no circumstances can non-public information be stored on portable devices such as PDAs, a thumb/flash drive or laptop unless the information is encrypted and access to the information is protected by a password established under the criteria established by the Firm. (See Retention and Back-up below.)

ANY BREACHES TO THESE PROCEDURES WILL RESULT IN PROMPT DISCIPLINARY ACTION.

4. Storage, Retention and Back-Up

Whenever possible, the Firm will seek to minimize the non-public information retained in its files. This can be done through a number of methods, including redacting all but the last 4 digits in a Social Security or credit card number or by not maintaining Social Security, credit card or other identifying numbers.

However, the Firm may be required to retain non-public information in its files for business or regulatory purposes.

In doing so, the Firm makes every effort to ensure that the information stored on its systems or in its paper files is secure.

The CCO and the Director of HR are responsible for ensuring that the Firm's policies related to the retention and storage of non-public information are followed.

SHOULD A BREACH OR UNAUTHORIZED ACCESS OCCUR, THE DESIGNATED PERSON IDENTIFIED ABOVE MUST IMMEDIATELY BE NOTIFIED. FAILURE TO PROVIDE NOTIFICATION WILL RESULT IN DISCIPLINARY ACTION.

The people previously identified shall ensure that any breach, misappropriation or loss of such information is immediately reported to:

- The individual(s) whose information was compromised, and
- Applicable state or federal regulatory or law enforcement agencies.

Failure by the Firm to report breaches to files containing non-public information or incidents of identity theft can result in civil and criminal actions against the Firm and the persons with knowledge of the breach or theft that did not report it.

4.1. Paper Documents

From the time paper documents containing non-public information are received by the Firm, they are maintained in a secure manner. To ensure the confidential retention of such files, the Firm has instituted the following procedures:

- All documents being used in work areas must be kept face down when not in use or if the person using the information steps away from his or her work area for a short period.
- All documents not being used for current work processes, or when the person processing the information leaves his or her work area for an extended period, must be locked in file cabinets or desk drawers.
- At the end of the work day, all documents containing non-public information must be removed from work surfaces and stored in locked cabinets containing applicable, related files.
- Only individuals who are required and authorized to receive and access information contained on paper documents may possess those documents or have access to files containing such information.

4.2. Electronic Storage

From the time non-public information is received electronically by the Firm, it must be maintained in a secure manner.

To ensure the Firm's computer systems and files contained thereon are protected from unauthorized access, the following procedures have been adopted:

a) Computer systems are password protected;

b) Passwords are confidential and may not be shared with others;

c) Servers and desktop computers will be protected through the use of firewall and anti-virus software, which will be set for automatic updates by the vendor to ensure that the most recent versions are maintained;

d) Passwords will contain a combination of numbers, letters and/or special characters and be between 6-10 characters in length;

e) Individuals will be required to change their password at least every 90 days;

f) Systems will automatically block access to users if the login and password combination are incorrect after five successive attempts;

g) Only persons requiring access to such information will receive access to files containing non-public information; and

h) All individuals with access to files containing non-public information will be subject to a background check.

When accessing files containing non-public information from a remote location, it is important that individuals use only secure connections in private locations or areas. Accessing information over unsecured networks in public locations, such as airports or hotels, can result in that information or those passwords being accessed by unauthorized persons.

The Firm strictly prohibits persons from accessing non-public information through non-secure networks or in public areas where information can be easily viewed by others.

The CCO will be responsible for maintaining passwords and will be responsible for resetting passwords should access become locked.

Under no circumstances can non-public information be stored on portable devices such as a thumb/flash drive or laptop unless the information is encrypted and access to the information is protected by a password established under the criteria established by the Firm.

Individuals who wish to maintain information on such devices must obtain permission from the CCO. If such devices are lost or stolen, the incident must be immediately reported to the designated person at the Firm so he or she can assess the potential damages and take steps to mitigate risks or report losses as applicable.

5. Disposal or Destruction of Information

Once the Firm has terminated the relationship with the individual from whom the non-public information was received or once the Firm is no longer required to maintain such information, it must be disposed of in a manner that ensures that its confidentiality is maintained.

The CCO is responsible for ensuring that the Firm's policies are followed relative to the destruction and disposal of paper or electronic files containing non-public information or devices on which such electronic files were stored.

SHOULD A BREACH OR UNAUTHORIZED ACCESS OCCUR, THE DESIGNATED PERSON IDENTIFIED ABOVE MUST BE NOTIFIED IMMEDIATELY. FAILURE TO PROVIDE NOTIFICATION WILL RESULT IN DISCIPLINARY ACTION.

The person previously identified shall ensure that any breach, misappropriation or loss of such information is immediately reported to:

- The individual(s) whose information was compromised, and
- Applicable state or federal regulatory or law enforcement agencies.

Failure by the Firm to report breaches to files containing non-public information or incidents of identity theft can result in civil and criminal actions against the Firm and the persons with knowledge of the breach or theft that did not report it.

5.1. Paper Files

The Firm will ensure all information is protected upon disposal by utilizing a cross-cut shredder to destroy all paper documents containing non-public information. Supervisors will periodically check offices and trash receptacles to ensure that information is not being disposed of improperly.

5.2. Electronic Files

Simply deleting a file from a computer, a shared server file or portable device does not remove all record of the file.

Therefore where a disk is being prepared for disposal, the Firm will ensure that any files containing non-public information to be removed from computer storage areas are removed by a qualified IT professional or company, as contracted by the Firm, who will scrub the drive to remove all traces of the files.

The Firm may periodically contract with an IT professional or service to test the integrity of these procedures by trying to retrieve previously disposed of information from electronic files.

FAILURE BY PERSONNEL TO DISPOSE OF PAPER OR ELECTRONIC DOCUMENTS, AS REQUIRED BY FIRM POLICIES, WILL RESULT IN IMMEDIATE DISCIPLINARY ACTION.

6. Use of Third Party Vendors

Firm makes use of third-party vendors to store or manage customer, employee or other data containing non-public information.

These outside vendors are identified in the Firm's WSP and the relationships with these vendors are the responsibility of the CCO.

Firm will ensure that each vendor they utilize that has access to non-public information has systems in place to protect this information and that a confidentiality agreement has been signed.

In addition, the Firm will require that the vendor provide a certification prior to contracting that outlines the processes and procedures the vendor has undertaken to protect confidential, non-public information, the testing procedures the vendor uses to ensure its systems are functioning properly, and the procedures and timeframes or notification the vendor uses if there are any breaches to these systems.

The Firm will also require that the vendor certify annually that testing has been undertaken, that no breaches have occurred, and that the firm's systems include the most up-to-date software and hardware for protecting its systems and data store thereon.

7. Termination

7.1. Employees or registered persons

Upon the termination or resignation of any employee or registered person, the designated manager or supervisor shall secure all keys, files, laptops or other Firm property from the individual.

At the same, all access to the Firm's computer systems used by the applicable person shall be immediately suspended such that that person cannot gain access to the system (such methods of achieving this include the changing of passwords, etc.).

In addition, if the employee or registered person had keys or security passcodes to access Firm offices, the locks and/or passcodes shall be changed or disabled to ensure that the individual can no longer access the premises.

7.2. Vendors

Upon the termination of any vendor relation, where the vendor had access to non-public personal information gathered or stored by the Firm, the Firm shall ensure that all access to such information is terminated and that any information in the vendors possession is immediately returned.

Failure of a vendor to return such information will result in a report being filed with the applicable state or federal agency regarding a potential breach.

8. Testing and Documentation

8.1. Testing

At least annually the applicable supervisory personnel at the Firm shall evaluate the integrity of the systems and procedures in place to protect non-public personal information gathered by the Firm to ensure that, in light of changing business needs, personnel, technology and other matters, the processes and procedures in place continue to meet the needs of the Firm and are adequate based on current regulations and the information being gathered and stored.

In addition, the designated managers or principals responsible for the information gathered in various areas of the Firm shall conduct reviews of the information security measures being undertaken in their applicable areas of supervision at least annually to ensure that procedures are being followed and the procedures remain adequate based on the current business needs and systems being employed.

When needed, changes will be made to the systems or procedures to ensure continuing compliance with applicable State or Federal rules and regulations and the security of non-public personal information gathered and maintained by the Firm.

8.2. Documentation

Reviews and remedial action taken, if needed, shall be documented and shall become part of the Firm's documentation relating to the annual testing of its policies and procedures

Further, the Firm shall maintain records of all potential, suspected or actual breaches including the circumstances surrounding the incident, the action taken to report the breach, if one occurred, and changes made to prevent future breaches.

Glossary

Term	Description
AA	Account Administrator
ACP	Address Confidentiality Programs
ACT	Automated Confirmation Transaction System
ADR	American Depository Receipt
AGU	Automated Give Up
AML	Anti-Money Laundering
AMLCP	AML Compliance Program
BCP	Business Continuity Plan
BDC	Business Development Company(ies)
C/E Principal	Continuing Education Principal
CCO	Chief Compliance Officer
CEO	Chief Executive Officer
CIP	Customer Identification Program
CRA	Consumer Reporting Agency(ies)
CRD	Central Registration Depository
DBA	Doing Business As
Designated Principal	Name of Supervisor
DRP	Disclosure Reporting Page
EAI	Estimated Annual Income
ECN	Electronic Communications Networks
EST	Eastern Standard Time
ETF	Exchange Traded Fund
EY	Estimated Yield
FCPA	Foreign Corrupt Practice Act of 1977

Term	Description
FCS	FINRA Contact System
FINRA	Financial Industry Regulatory Authority
Firm	Peel Hunt Inc.
Form BD	Broker Dealer Registration Form
Form BR	Uniform Branch Registration Form
FRP	Free Writing Prospectus
FTD	Fail to Deliver
HR	Human Resources
IA	Investment Advisor
IPO	Initial Public Offering
IT	Information Technology
ITPP	Identity Theft Prevention Program
KYC	Know Your Customer
MSRB	Municipal Securities Rulemaking Board
NAF	New Account Form
NBBO	National Best Bid or Offer
NYSE	New York Stock Exchange
OATS	Order Audit Trail System
OBA	Outside Business Activities
OFAC	Office of Foreign Assets Control
ORF	OTC Reporting Facility
OSJ	Office of Supervisory Jurisdiction
OTC	Over-the-Counter
QSR	Qualified Service Representative
RFA	Regulation Filing Applications

Term	Description
RR	Registered Representatives
SAA	Super Account Administrator
SEC	Securities & Exchange Commission
Selling Away	Private Securities Transactions
SIPC	Securities Investor Protection Corporation
SIPA	Securities Investor Protection Act
SNS	Social Media Sites
SRO	Self-Regulatory Organisation
SSN	Social Security Number
TIN	Taxpayer Identification Number
WSP	Written Supervisory Procedures Manual