TRITON WEALTH MANAGEMENT, PLLC

IDENTITY THEFT PREVENTION PROGRAM ("ITPP")

Triton Wealth Management, PLLC's ("TWM") policy is to protect its clients from identity theft and to comply with the SEC's Red Flags Rule. This will be done by developing and implementing this written ITPP, which serves as a supplement to TWM's existing policies and procedures. This policy is meant to establish procedures that will: (1) identify relevant identity theft Red Flags; (2) detects Red Flags; and (3) mitigate Red Flags when detected.

TWM's identity theft policies, procedures and internal controls will be reviewed and updated periodically to ensure they account for changes both in regulations and in our business.

Rule: 17 CFR part 248, Regulation S-ID: Identity Theft Red Flags Rules, Section II.A.III.

ITPP Approval & Administration

TWM's owners have approved this ITPP. Cody Ashton is the designated contact and is responsible for the oversight, development, implementation and administration (including staff training and oversight of third party service providers of ITTP services) of the ITPP.

Identifying Relevant Red Flags

TWM considers the following risk factors when identifying relevant red flags for covered accounts:

- the types of covered accounts offered;
- the methods provided to open or access these accounts; and
- previous experiences with identity theft.

In addition, Red Flags from the following five categories and the attached "Red Flag Identification & Detection Grid" ("Grid") have been considered:

- alerts, notifications, or warnings from a credit reporting agency or service providers;
- presentation of suspicious documents;
- presentation of suspicious personal identifying information;
- unusual use of, or other suspicious activity related to a covered account; and
- notice from other clients, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.

It should be noted that the examples listed in the "Red Flag Identification & Detection Grid" are not exhaustive, nor do they constitute a mandatory checklist, but should be utilized as a resource of relevant red flags in the context of the business.

Rule: 17 CFR part 248, Regulation S-ID: Identity Theft Red Flags Rules, Sec II. B. II.

Detecting Red Flags

TWM will review the opening and maintenance procedures for covered accounts in order to detect Red Flags. For opening covered accounts, which can include obtaining identifying information, TWM will verify the identity of the person opening the account and request relevant supporting documentation. For existing covered accounts, TWM will verify client's identity, monitor transactions, and verify the validity of changes that are requested.

Rule: 17 CFR part 248, Regulation S-ID: Identity Theft Red Flags Rules, Sec II.B.III.

Preventing & Mitigating Identity Theft

Based on the Red Flags that have been detected and the suggested responses for mitigating identity theft, the following procedures have been developed to respond to detected identity theft Red Flags. When TWM has been notified of a Red Flag or detection procedures show evidence of a Red Flag, the following steps will be taken, as appropriate to the type and seriousness of the threat:

I. Applicants (*Red Flags raised by someone applying for an account*)

Review the Application. TWM will review the applicant's information collected for opening an account (e.g., name, date of birth, address, and an identification number such as a Social Security Number or Taxpayer Identification Number).

Request Government Identification. If the applicant is applying in person, a current government-issued identification card, such as a driver's license or passport will be checked.

Seek Additional Verification. If the risk of identity theft is probable or large in impact, TWM may also verify the person's identity through non-documentary methods, including:

- Contacting the applicant through the contact information provided;
- Independently verifying the client's information by comparing it with information from a credit reporting agency, public database or other source such as a data broker or the Social Security Number Death Master File;
- Checking references with other affiliated financial institutions, or
- Obtaining a financial statement.

Deny the Application. If the applicant is found using an identity other than his or her own, the account will be denied.

Report. If the applicant is found using an identity other than his or her own, TWM will report it to appropriate local and state law enforcement; where organized or wide spread crime is suspected, the FBI or Secret Service; and if mail is involved, the US Postal Inspector. It may also, as recommended by FINRA's Customer Information Protection web page's "Firm Checklist for Compromised Accounts," be reported to the appropriate FINRA coordinator; the SEC; State regulatory authorities, such as the state securities commission; and TWM's clearing firm.

Notification. If determined that personal identifiable information has been accessed, TWM will prepare any specific notice or any other required notice under state law to clients.

II. Access Seekers (*Red Flags raised by someone seeking access to an existing client's account*)

Watch. TWM will monitor, limit, or temporarily suspend activity in the account until the situation is resolved.

Check with the Client. TWM will contact the client, describe what was found and verify with them that there has been an attempt at identify theft.

Heightened Risk. TWM will determine if there is a particular reason that makes it easier for an intruder to seek access, such as a client's lost wallet, mail theft, a data security incident, or the client's giving account information to an imposter pretending to represent the firm or to a fraudulent web site.

Check Similar Accounts. TWM will review similar accounts under management to see if there have been attempts to access them without authorization.

Collect Incident Information. For a serious threat of unauthorized account access TWM may, as recommended by FINRA's Customer Information Protection web page's "Firm Checklist for Compromised Accounts," collect if available:

- Firm information (both introducing and clearing firms): Firm name, CRD number, contact name & telephone number
- Dates and times of activity
- Securities involved (name and symbol)
- Details of trades or unexecuted orders
- Details of any wire transfer activity
- Client accounts affected by the activity, including name and account number, and
- Whether the client will be reimbursed and by whom.

Report. If unauthorized account access is found, TWM will report it to appropriate local and state law enforcement; where organized or wide spread crime is suspected, the FBI or Secret Service; and if mail is involved, the US Postal Inspector. TWM may also, as recommended by FINRA's Customer Information Protection web page's "Firm Checklist for Compromised Accounts," report it to their FINRA coordinator; the SEC; State regulatory authorities, such as the state securities commission; and their clearing firm.

Notification. If determined that personal identifiable information has been accessed that results in a foreseeable risk for identity theft, TWM will prepare any specific notice to clients or other required under state law.

Review of Insurance Policy. Since insurance policies may require timely notice or prior consent for any settlement, we will review our insurance policy to ensure that their response to a data breach does not limit or eliminate our insurance coverage.

Assist the Client. We will work with our clients to minimize the impact of identity theft by taking the following actions, as applicable:

- Offering to change the password, security codes or other ways to access the threatened account;
- Offering to close the account;
- Offering to reopen the account with a new account number;
- Not collecting on the account or selling it to a debt collector; and
- Instructing the client to go to the FTC Identity Theft Web Site to learn what steps to take to recover from identity theft, including filing a complaint using its online complaint form, calling the FTC's Identity Theft Hotline 1-877-ID-THEFT (438-4338), TTY 1-866-653-4261, or writing to Identity Theft Clearinghouse, FTC, 6000 Pennsylvania Avenue, NW, Washington, DC 20580.

Rule: 17 CFR part 248, Regulation S-ID: Identity Theft Red Flags Rules, Sec II.B.IV.

Clearing Firm & Other Service Providers

TWM engages other service providers to perform activities in connection with covered accounts, who we reasonably believe conduct in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

Annual Review & Reporting

The designated identity theft officer review and update this ITPP on at least an annual basis or as needed, depending on the following factors to:

- Recent experiences with identity theft;
- Changes in methods of identity theft;
- Changes in methods to detect, prevent, and mitigate identity theft;
- Changes in the types of accounts that TWM offers or maintains;
- Changes in service provider arrangements.

The designated identity theft officer will report to TWM's principal(s) on at least an annual basis or as needed, to address material matters related to the ITPP. The report will address the effectiveness of the ITPP in addressing the risk of identity theft in connection with covered account, significant incidents involving identity theft, and management's response and recommendations for material changes to the ITPP.

Rule: 17 CFR part 248, Regulation S-ID: Identity Theft Red Flags Rules, Sec.II.B.6.ii.

Approval

I approve this ITPP as reasonably designed to enable TWM to detect, prevent and mitigate identity theft.

Rule: 17 CFR part 248, Regulation S-ID: Identity Theft Red Flags Rules, Sec.II.A.4. 114.

_____ _____

Signature Date

_____

Print Name

RED FLAG IDENTIFICATION & DETECTION GRID

Red Flag	Detecting the Red Flag
Category: Alerts, Notifications or Warnings from a Consumer Credit Reporting Agency **Category: Suspicious Documents**	
1. Identification presented looks altered or forged.	TWM will scrutinize identification presented in person to make sure it is not altered or forged.
2. The identification presenter does not look like the identification's photograph or physical description.	TWM will ensure that the photograph and the physical description on the identification match the person presenting it.
3. Information on the identification differs from what the identification presenter is saying.	TWM will ensure that the identification and the statements of the person presenting it are consistent.
4. Information on the identification does not match other information TWM has on file for the presenter, like the original account application, signature card or a recent check.	TWM will ensure that the identification presented and other information we have on file from the account, such as the address on their driver's license are consistent.
5. The application looks like it has been altered, forged or torn up and reassembled.	TWM will scrutinize each application to make sure it is not altered, forged, or torn up and reassembled.
Category: Suspicious Personal Identifying Information	
6. Inconsistencies exist between the information presented and other things known or can find out about the presenter by checking readily available external sources.	TWM will check personal identifying information presented to us to ensure that the SSN given has been issued but is not listed on the SSA's Master Death File. If we receive a consumer credit report, they will check to see if the addresses on the application and the consumer report match.
7. Personal identifying information presented has been used on an account TWM knows was fraudulent.	TWM will compare the information presented with addresses and phone numbers on accounts or applications found or were reported to be fraudulent.
8. Personal identifying information presented suggests fraud, such as an address that is fictitious, a mail drop, or a prison; or a phone number is invalid, or is for a pager or answering service.	TWM will validate the information presented when opening an account by looking up addresses on the Internet to ensure they are real and not for a mail drop or a prison, and will call the phone numbers given to ensure they are valid and not for pagers or answering services.
9. The SSN presented was used by someone else opening an account or other clients.	TWM will compare the SSNs presented to see if they were given by others opening accounts or other clients.
10. The address or telephone number presented has been used by many other people opening accounts or other clients.	TWM will compare address and telephone number information to see if they were used by other applicants and clients.
11. A person who omits required information on an application or other form does not provide it when told it is incomplete.	TWM will track when applicants or clients have not responded to requests for required information and will follow up with the applicants or clients to determine why they have not responded.
12. Inconsistencies exist between what is presented and on TWM's file.	TWM will verify key items from the data presented with information they have on file.
13. A person making an account application or seeking access cannot provide authenticating information beyond what would be found in a wallet or consumer credit report, or cannot answer a challenge question.	TWM will authenticate identities for existing clients by asking challenge questions that have been prearranged with the client and for applicants or clients by asking questions that require information beyond what is readily available from a wallet or a consumer credit report.
Category: Suspicious Account Activity	
14. Soon after TWM gets a change of address request for an account, they are asked to add additional access means (such as debit cards or checks) or authorized	TWM will verify change of address requests by sending a notice of the change to both the new and old addresses so the client will learn of any unauthorized changes and can

users for the account.	notify TWM.
15. A new account exhibits fraud patterns, such as where a first payment is not made or only the first payment is made, or the use of credit for cash advances and securities easily converted into cash.	TWM will review new account activity to ensure that first and subsequent payments are made, and that credit is primarily used for other than cash advances and securities easily converted into cash.
16. An account develops new patterns of activity, such as nonpayment inconsistent with prior history, a material increase in credit use, or a material change in spending or electronic fund transfers.	TWM will review their accounts on at least a monthly basis and check for suspicious new patterns of activity such as nonpayment, a large increase in credit use, or a big change in spending or electronic fund transfers.
17. An account that is inactive for a long time is suddenly used again.	TWM will review their accounts on at least a monthly basis to see if long inactive accounts become very active.
18. Mail TWM sends to a client is returned repeatedly as undeliverable even though the account remains active.	TWM will note any returned mail for an account and immediately check the account's activity.
19. TWM learns that a client is not getting his or her paper account statements.	TWM will record on the account any report that the client is not receiving paper statements and immediately investigate them.
20. TWM is notified that there are unauthorized charges or transactions to the account.	TWM will verify if the notification is legitimate and involves a firm account, and then investigate the report.
Category: Notice From Other Sources	
21. TWM is told that an account has been opened or used fraudulently by a client, an identity theft victim, or law enforcement.	TWM will verify that the notification is legitimate and involves a firm account, and then investigate the report.
22. TWM learns that unauthorized access to the client's personal information took place or became likely due to data loss (e.g., loss of wallet, birth certificate, or laptop), leakage, or breach.	TWM will contact the client to learn the details of the unauthorized access to determine if other steps are warranted.