Identity Theft Policies and Procedures

Davis & Wehrle, LLC

1104 S. Mays, Suite 105
Round Rock, TX 78664-6700
United States

(512) 346-1131

Table of Contents

Firm Policy

Pursuant to Rule: 16 C.F.R. § 681.1(d), our firm's policy is to protect our customers and their accounts from identity theft and to comply with the FTC's Red Flags Rule. Davis & Wehrle, LLC ("Davis & Wehrle") will do this by developing and implementing these written Identity Theft Policies and Procedures (ITPP), which have been tailored to fit our size and complexity, as well as the nature and scope of our activities. These procedures address:

- Identifying applicable identity theft Red Flags for our firm
- How we will detect those Red Flags
- Responding appropriately to any that are detected
- Updating our ITPP periodically to reflect changes in risks

Our 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 model.

The definitions of the abbreviations used throughout this document are listed below:

Abbreviation	Definition
ITPP	Identity Theft Policies and Procedures
CIP	Client Identification Procedures
AML	Anti-Money Laundering
FTC	Federal Trade Commission

ITPP Approval and Administration

Pursuant to Rule: 16 C.F.R. § 681.1(e) and Appendix A, Section VI.(a), approved the initial ITPP and is the designated identity theft officer 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.

Relationship to Other Firm Programs

Pursuant to Rule: 16 C.F.R. § 681.1, Appendix A, Section I, we have reviewed our other policies, procedures and plans required by regulations regarding the protection of our customer information, including our policies and procedures and our CIP and red flags detection under our AML Compliance Program in the formulation of the ITPP.

Identifying Relevant Red Flags

Pursuant to Rule: 16 C.F.R. § 681.1(d)(2)(i) and Appendix A, Section II, which requires Davis & Wehrle to identify Red Flags applicable to our firm, we assessed these risk factors:

- The types of covered accounts we offer
- The methods used to open or access these accounts
- All previous experiences with identity theft
- Changing identity theft techniques
- Applicable supervisory guidance

In addition, we considered Red Flags from the following five categories and from the FTC's Red Flags Rule, as they fit our situation:

- Alerts, notifications or warnings from a credit reporting agency
- Suspicious documents
- Suspicious personal identifying information
- Suspicious account activity
- Notices from other sources

Detecting Red Flags

Pursuant to Rule: 16 C.F.R. § 681.1(d)(2)(ii) and Appendix A, Section III, we have reviewed our client accounts, how we open and maintain them, and how to detect Red Flags that may have occurred in them. Our detection of these Red Flags is based on our methods of obtaining information about our clients and verifying it under the CIP of our AML compliance procedures, authenticating customers and monitoring transactions and change of address requests. Account opening procedures include gathering identifying information about and verifying the identity of the person opening the account by using the firm's CIP. Review of existing accounts includes authenticating customers, monitoring transactions, and verifying the validity of changes of address. Based on this review, we have included in the second column ("Detecting the Red Flag") of the attached Grid how we will detect each of our firm's identified Red Flags.

Our CCO reviews, at least annually, our covered accounts, how we open and maintain them, and how to detect Red Flags.

Preventing and Mitigating Identity Theft

Pursuant to Rule: 16 C.F.R. § 681.1(d)(iii) and Appendix A, Section IV, we have reviewed our accounts, how we open and allow access to them, and our previous experience with identity theft, as well as any new methods of identity theft we have seen or believe to be likely. Based on these reviews and our review of the FTC's identity theft rules and its suggested responses to mitigate identity theft, as well as other sources, we have developed our procedures below to respond to detected identity theft Red Flags.

Procedures to Prevent and Mitigate Identity Theft

When we have been notified of a Red Flag or our detection procedures show evidence of a Red Flag, we will take the steps outlined below, as appropriate to the type and seriousness of the threat:

New Accounts

Procedures when Red Flags raised by someone applying for an account:

- Review the application.
    - We will review the applicant's information collected for our CIP under our AML Compliance Program (e.g., name, date of birth, address, and an identification number such as a Social Security Number or Taxpayer Identification Number).
- Get government identification.
    - If the applicant is applying in person, we will also check a current government-issued identification card, such as a driver's license or passport.
- Seek additional verification.

- If the potential risk of identity theft indicated by the Red Flag is probable or large in impact, we may also verify the person's identity through non-documentary CIP methods, including:
    - Contacting the customer
    - Independently verifying the customer'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
    - Obtaining a financial statement
- Deny the application.
    - If we find that the applicant is using an identity other than his or her own, we will deny the account and report the incident to the appropriate authorities.
- Report.
    - If we find that the applicant is using an identity other than his or her own, we 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.
- Notification.
    - If we determine personally identifiable information has been accessed, we will prepare any specific notice to customers or other required notice under state law.

Access Seekers

For Red Flags raised by someone seeking to access an existing customer's account:

- Watch.
    - We will monitor, limit, or temporarily suspend activity in the account until the situation is resolved.
- Check with the customer.
    - We will contact the customer by phone using our CIP information for them, describe what we have found and verify with them that there has been an attempt at identify theft.
- Heightened risk.
    - We will determine if there is a particular reason that makes it easier for an intruder to seek access, such as a customer's lost wallet, mail theft, a data security incident, or the customer's giving account information to an imposter pretending to represent the firm or to a fraudulent web site.
- Check similar accounts.
    - We will review similar accounts the firm has to see if there have been attempts to access them without authorization.
- Collect incident information.
    - For a serious threat of unauthorized account access we may collect if available:
        - Firm information (both introducing and clearing firms):
            - ❖ Firm name and CRD number
            - ❖ Firm contact name and telephone number
        - Dates and times of activity
        - Securities involved (name and symbol)
        - Details of trades or unexecuted orders
        - Details of any wire transfer activity
        - Customer accounts affected by the activity, including name and account number

        - Whether the customer will be reimbursed and by whom
- Report.
    - If we find unauthorized account access, we 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. We may also report it to the SEC, State regulatory authorities such as the state securities commission; and our clearing/custodian firm.
- Notification.
    - If we determine personally identifiable information has been accessed that results in a foreseeable risk for identity theft, we will prepare any specific notice to customers and appropriate agencies as required under state law.
- Review our insurance policy.
    - Since insurance policies may require timely notice or prior consent for any settlement, we will review our insurance policy to ensure that our response to a data breach does not limit or eliminate our insurance coverage.
- Assist the customer.
    - We will work with our customers 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
        - Instructing the customer 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.

Clearing Firm and Other Service Providers

Our firm uses a custodian in connection with our accounts. We have a process to confirm that our clearing/custodian firm and any other service provider that performs activities in connection with our covered accounts, especially other service providers that are not otherwise regulated, comply with reasonable policies and procedures designed to detect, prevent and mitigate identity theft by contractually requiring them to have policies and procedures to detect Red Flags contained in our Grid and report detected Red Flags to us or take appropriate steps of their own to prevent or mitigate the identify theft or both. This process includes, at least annually, verifying the existence of each vendor's privacy policy and/or identity theft policy and procedures and maintaining them in designated files. Our list of service providers that perform these activities in connection with our covered accounts include:

1. **TD Ameritrade**
   www.tdameritrade.com
   1-800-669-3900

2. **Charles Schwab & Company**
   www.schwab.com

1-866-855-9102

Internal Compliance Reporting

Pursuant to Rule: 16 C.F.R. § 681.1, Appendix A, Section VI.(b), our firm's staffs who are responsible for developing, implementing and administering our ITPP will report at least annually to our CCO on compliance with the FTC's Red Flags Rule. The report will address the effectiveness of our ITPP in addressing the risk of identity theft in connection with covered account openings, existing accounts, and service provider arrangements, significant incidents involving identity theft and management's response and recommendations for material changes to our ITPP.

Updates and Annual Review

Pursuant to Rule: 16 C.F.R. § 681.1 (d)(2)(iv) and Appendix A, Sections V. and VI. (a) & (b), we will update this plan whenever we have a material change to our operations, structure, business or location or to those of our clearing firm, or when we experience either a material identity theft from a covered account, or a series of related material identity thefts from one or more covered accounts. Our firm will also follow new ways that identities can be compromised and evaluate the risk they pose for our firm. In addition, our firm will review this ITPP annually to modify it for any changes in our operations, structure, business, or location or substantive changes to our relationship with our custodians or service providers.

Approval

I approve this ITPP as reasonably designed to enable our firm to detect, prevent and mitigate identity theft. This approval is indicated by signature below.

Kevin T. Davis _____ 09/27/2017 _____

Date

Appendix A: Red Flag Identification and Detection Grid

This grid provides FTC categories and examples of potential red flags that are applicable to our firm.

Red Flag	Detecting the Red Flag
Alerts, Notifications or Warnings from a Consumer Credit Reporting Agency	
A fraud or active duty alert is included on a consumer credit report.	We do not usually run credit reports on clients but may run credit reports on our employees. However we will verify whether the alert covers a customer and review the allegations in the alert if this occurs.
A notice of credit freeze is given in response to a request for a consumer credit report.	We do not usually run credit reports on our clients but may run credit reports on our employees. We will verify whether the credit freeze covers a customer and review the freeze.
A notice of address or other discrepancy is provided by a consumer credit reporting agency.	We do not usually run credit reports on our clients but may run credit reports on employees. We will verify whether the notice of address or other discrepancy covers a customer and review the address discrepancy.
A consumer credit report shows a pattern inconsistent with person's history, i.e. increase in the volume of inquiries or use of credit; an unusual number of recently established credit relationships; or an account closed due to an abuse of account privileges.	We do not usually run credit reports on our clients but may run credit reports on our employees. However, we will verify whether the consumer credit report covers an applicant or customer, and review the degree of inconsistency with prior history.
Suspicious Documents	
Identification presented looks altered or forged.	We will scrutinize identification presented in person to make sure it is not altered or forged. If it does look altered or forged, it will be brought to the attention of the CCO.
The identification presenter does not look like the identification's photograph or physical description.	We will ensure the photograph and physical description on the identification matches the person presenting it. Any questions will be brought to the attention of the CCO.
Information on the identification differs from what the identification presenter is saying.	We will ensure the identification and statements of the person presenting it are consistent. If there is any question about its authenticity, it will be brought to the attention of the CCO.
Information on the identification does not match other information our firm has on file for the presenter, like the original account application, signature, etc.	We will ensure that the identification presented and other information we have on file from the account, such as the application is consistent. Additional information and sources may need to be contacted for verification.
The application looks like it has been altered, forged or torn up and reassembled.	We will scrutinize each application to make sure it is not altered, forged, or torn up and reassembled. If there is any question about its authenticity, it will be brought to the attention of the CCO.
Suspicious Personal Identifying Information	

Inconsistencies exist between the information presented and other things known about the presenter or can find out by checking readily available external sources, such as an address that does not match a consumer credit report, or the Social Security Number (SSN) has not been issued or is listed on the Social Security Administration's Death Master File.	We 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, we will check to see if the addresses on the application and the consumer credit report match.
Inconsistencies exist in the information that the customer gives us, such as a date of birth that does not fall within the number range on the SSA's issuance tables.	We will check personal identifying information presented to us to make sure that it is internally consistent by comparing the date of birth to see that it falls within the number range on the SSA's issuance tables.
Personal identifying information presented has been used on an account our firm knows was fraudulent.	We will compare the information presented with addresses and phone numbers on accounts or applications we found or were reported as fraudulent. Any questions will be brought to the attention of the CCO.
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.	We 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. Any questions will be brought to the attention of the CCO.
The SSN presented was used by someone else opening an account or other customers.	We will compare the SSNs presented to see if they were given by others opening accounts or other customers. Any questions will be brought to the attention of the CCO.
The address or telephone number presented has been used by many other people opening accounts or other customers.	We will compare address and telephone number information to see if they were used by other applicants and customers. Any questions will be brought to the attention of the CCO.
A person who omits required information on an application or other form does not provide it when told it is incomplete.	We will track when applicants or customers have not responded to requests for required information and will follow up with the applicants or customers to determine why they have not responded. Any questions will be brought to the attention of the CCO.
Inconsistencies exist between what is presented and what our firm has on file.	We will verify key items from the data presented with information we have on file. Any questions will be brought to the attention of the CCO.
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.	We will authenticate identities for existing customers by asking challenge questions that require information beyond what is readily available from a wallet or a consumer credit report. Any questions will be brought to the attention of the CCO.
Suspicious Account Activity	

Soon after our firm gets a change of address request for an account, we are asked to add additional access means (such as debit cards or checks) or authorized users for the account.	The custodian will verify change of address requests by sending a notice of the change to both the new and old addresses so the customer will learn of any unauthorized changes and can notify us.
An account develops new patterns of activity, such as a material increase in credit use, or a material change in spending or electronic fund transfers.	We will review our 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.
An account that is inactive for a long time is suddenly used again.	We will review our accounts on at least a monthly basis to see if long inactive accounts become very active.
Mail our firm sends to a customer is returned repeatedly as undeliverable even though the account remains active.	We will note any returned mail for an account and immediately check the account's activity. Any questions will be brought to the attention of the CCO.
We learn that a customer is not getting his or her paper account statements.	We will record on the account any report that the customer is not receiving paper statements and immediately investigate them and notify the custodian to place a watch on the account or close the account and reopen a new one if necessary.
We are notified that there are unauthorized charges or transactions to the account.	We will verify if the notification is legitimate and involves a firm account, and then investigate the report. We will notify the custodian to place a watch on the account or close the account and reopen a new one if necessary.
Notice From Other Sources	
We are told that an account has been opened or used fraudulently by a customer, an identity theft victim, or law enforcement.	We will verify that the notification is legitimate and involves a firm account, and then investigate the report. We will notify the custodian to place a watch on the account or close the account and reopen a new one if necessary.
We learn that unauthorized access to the customer's personal information took place or became likely due to data loss (e.g., loss of wallet, birth certificate, or laptop), leakage, or breach.	We will contact the customer to learn the details of the unauthorized access to determine if other steps are warranted. We will notify the custodian to place a watch on the account or close the account and reopen a new one if necessary. If the loss is a result of the firm's breach or leakage, appropriate steps will be taken to rectify the situation and the appropriate law and regulatory authorities notified.