



Identity Theft Prevention Program (ITPP) under the FTC FACT Act Red Flags Rule

I. Firm Policy

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. We will do this by developing and implementing this written ITPP, which is appropriate to our size and complexity, as well as the nature and scope of our activities. This ITPP addresses 1) identifying relevant identity theft Red Flags for our firm, 2) detecting those Red Flags, 3) responding appropriately to any that are detected to prevent and mitigate identity theft, and 4) 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.

Rule: 16 C.F.R. § 681.1(d).

II. ITPP Approval and Administration

The firm's Executive Committee has approved this initial ITPP. Paul Chuzi, Chief Compliance Officer, a member of senior management, 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 this ITPP.

Rule: 16 C.F.R. § 681.1(e) and Appendix A, Section VI.(a).

III. Relationship to Other Firm Programs

We have reviewed other policies, procedures and plans required by regulations regarding the protection of our customer information, including our policies and procedures under Regulation S-P, and our CIP and red flags detection under our AML Compliance Program in the formulation of this ITPP, and modified either them or this ITPP to minimize inconsistencies and duplicative efforts.

Rule: 16 C.F.R. § 681.1, Appendix A, Section I.

IV. Identifying Relevant Red Flags

To identify relevant identity theft Red Flags, our firm assessed these risk factors: 1) the types of covered accounts it offers, 2) the methods it provides to open or access these accounts, and 3) previous experience with identity theft. Our firm also considered the sources of Red Flags, including identity theft incidents our firm has experienced, changing identity theft techniques our firm thinks likely, and applicable supervisory guidance. In addition, we considered Red Flags from the following five categories (and the 26 numbered examples under them) from Supplement A to Appendix A of the FTC's



Red Flags Rule, as they fit our situation: 1) alerts, notifications or warnings from a credit reporting agency; 2) suspicious documents; 3) suspicious personal identifying information; 4) suspicious account activity; and 5) notices from other sources. We understand that some of these categories and examples may not be relevant to our firm and some may be relevant only when combined or considered with other indicators of identity theft. We also understand that the examples are not exhaustive or a mandatory checklist, but a way to help our firm think through relevant red flags in the context of our business. Based on this review of the risk factors, sources, and FTC examples of red flags, we have identified our firm's Red Flags, which are contained the first column ("Red Flag") of the attached "Red Flag Identification and Detection Grid" ("Grid").

Rule: 16 C.F.R. § 681.1(d)(2)(i) and Appendix A, Section II.

V. Detecting Red Flags

We have reviewed our covered accounts, how we open and maintain them, and how to detect Red Flags that may have occurred in them. Our detection of those Red Flags is based on our methods of getting information about applicants and verifying it under our CIP of our AML compliance procedures, authenticating customers who access the accounts, and monitoring transactions and change of address requests. For opening covered accounts, that can include getting identifying information about and verifying the identity of the person opening the account by using the firm's CIP. For existing covered accounts, it can include 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.

Rule: 16 C.F.R. § 681.1(d)(2)(ii) and Appendix A, Section III.

VI. Preventing and Mitigating Identity Theft

We have reviewed our covered accounts, how we open and allow access to them, and our previous experience with identity theft, as well as new methods of identity theft we have seen or foresee as likely. Based on this 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:

Applicants. For Red Flags raised by someone applying for an account:

1. **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).
2. **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.
3. **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:
 - a. Contacting the customer



- b. 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 [or *list other sources*]
 - c. Checking references with other affiliated financial institutions, or
 - d. Obtaining a financial statement.
4. Deny the application. If we find that the applicant is using an identity other than his or her own, we will deny the account.
 5. 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. We may also, as recommended by FINRA's Customer Information Protection web page's "Firm Checklist for Compromised Accounts," report it to our FINRA coordinator; the SEC; State regulatory authorities, such as the [state securities commission](#); and our clearing firm.
 6. 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:

1. Watch. We will monitor, limit, or temporarily suspend activity in the account until the situation is resolved.
2. Check with the customer. We will contact the customer using our CIP information for them, describe what we have found and verify with them that there has been an attempt at identify theft.
3. 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.
4. Check similar accounts. We will review similar accounts the firm has to see if there have been attempts to access them without authorization.
5. Collect incident information. For a serious threat of unauthorized account access we may, as recommended by FINRA's Customer Information Protection web page's "Firm Checklist for Compromised Accounts," collect if available:
 - a. Firm information (both introducing and clearing firms):
 - i. Firm name and CRD number
 - ii. Firm contact name and telephone number
 - b. Dates and times of activity
 - c. Securities involved (name and symbol)
 - d. Details of trades or unexecuted orders
 - e. Details of any wire transfer activity
 - f. Customer accounts affected by the activity, including name and account number, and
 - g. Whether the customer will be reimbursed and by whom.
6. 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, as recommended by FINRA's Customer Information Protection web page's "Firm Checklist for Compromised Accounts," report it to our FINRA coordinator; the SEC; State regulatory authorities, such as the [state securities commission](#); and our clearing firm.
7. 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 or other required under state law. [see note at 6, under "[Applicants](#)" above]

8. 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.

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

- a. Offering to change the password, security codes or other ways to access the threatened account;
- b. Offering to close the account;
- c. Offering to reopen the account with a new account number;
- d. Not collecting on the account or selling it to a debt collector; and
- e. 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.

[Rule: 16 C.F.R. § 681.1\(d\)\(iii\) and Appendix A, Section IV.](#)

VII. Clearing Firm and Other Service Providers

Our firm uses a clearing firm *and other service providers* in connection with our covered accounts. We have a process to confirm that our clearing 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. Our clearing firms are:

1. Legent Clearing, Inc 9300 Underwood Ave. Suite 400 Omaha, NE 68114 (800) 811-3487 contact Ray Maratea Ray.Maratea@legentclearing.com.
2. Penson Financial Services 1700 Pacific Ave. Suite 1400 Dallas, TX 75201 (214) 765-1100 contact Amanda McCutcheon: amccutcheon@penson.com
3. RBC Correspondent Services, Inc. 60 South 6th St. Minneapolis, MN 55402 (866) 506-8595 Attn: Sandy K. Johnson. sandy.k.johnson@rbc.com

Our other service providers that perform activities in connection with our covered accounts are:

1. RemitPro RiskAlert Background Verification 3925 S. 147th St. Suite 117 Omaha, NE (877) 861-0005 Contact info@remitpro.com
2. McDonald Information Systems (MIS) 215 14th St. Jersey City, NJ (201) 659-2600 Contact: info@callmis.com.

[Rule: 16 C.F.R. § 681.1\(e\)\(4\) and Appendix A, Section VI.\(c\).](#)

VIII. Internal Compliance Reporting

Our firm's staffs who are responsible for developing, implementing and administering our ITPP will report at least annually to our Board *or* Paul Chuzi 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.

[Rule: 16 C.F.R. § 681.1, Appendix A, Section VI.\(b\).](#)



IX. Updates and Annual Review

Our firm 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, on August 1st, to modify it for any changes in our operations, structure, business, or location or substantive changes to our

relationship with our clearing firm.

[Rule: 16 C.F.R. § 681.1 \(d\)\(2\)\(iv\) and Appendix A, Sections V. and VI. \(a\) & \(b\).](#)

X. Approval

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

[Rule: 16 C.F.R. § 681.1 \(e\)\(1\)&\(2\) and Appendix A, Section VI.\(a\).](#)

Signed: Paul Chuzi
Title: Chief Compliance Officer
Date: March 1, 2010

ATTACHMENT: Red Flag Identification and Detection Grid (Grid)



RED FLAG IDENTIFICATION AND DETECTION GRID

RED FLAG	DETECTING THE RED FLAG
Category: Suspicious Documents	
1. Identification presented looks altered or forged.	Our staff who deals with customers, and their supervisors, 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.	Our staff who deals with customers, and their supervisors, 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.	Our staff who deals with customers, and their supervisors, 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 our firm has on file for the presenter, like the original account application, signature card or a recent check.	Our staff who deals with customers, and their supervisors, will ensure that the identification presented and other information we have on file from the account, such as Corporate or Trust documents, etc. are consistent.
5. The application looks like it has been altered, forged or torn up and reassembled.	Our staff who deals with customers, and their supervisors, 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 we know 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 (SSA's) Master Death File.	Our staff 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 address on the application and the consumer report match.
7. Inconsistencies exist in the information that the customer gives us, such as a date of birth that does not fall with the number range on the SSA's issuance tables.	Our staff 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 using RemitPro Background Verification Services.
8. Personal identifying information presented has been used on an account our firm knows was fraudulent.	Our staff will compare the information presented with addresses and phone numbers on accounts or applications we found or were reported were fraudulent. In addition, we will utilize the Internet, such as www.411.com or



	www.whitepages.com to verify address and phone information.
9. Personal identifying information presented suggest 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.	Our staff will validate the information presented when opening an account by looking up addresses on the Internet to insure 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.
10. The SSN presented was used by someone else opening an account or other customers.	Our staff will compare the SSNs presented to see if they were given by others opening accounts or other customers.
11. The address or telephone number presented has been used by many other people opening accounts or other customers.	Our staff will compare address and telephone number information to see if they were used by other applicants and customers.
12. A person who omits required information on an application or other form does not provide it when told it is incomplete.	Our staff 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.
13. Inconsistencies exist between what is presented and what our firm has on file.	Our staff will verify key items from the data presented with information we have on file.
14. 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.	Our staff will authenticate identities for existing customers by asking challenge questions that have been prearranged with the customer and for applicants or customers by asking questions that require information beyond what is readily available from a wallet or a consumer credit report.
Category: Suspicious Account Activity	
15. 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.	We 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.
16. 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.	We 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.
17. 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.	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.
18. 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.
19. Mail our firm sends to a customer is returned repeatedly as undeliverable even though the account remains active.	We will not any returned mail for an account and immediately check the account's activity.
20. We learn that a customer is not getting his	We will record on the account any report that



or her paper account statements.	the customer is not receiving paper statements and immediately investigate them.
21. 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.
Category: Notice From Other Sources	
22. 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 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.