CASTLEBERRY TELEPHONE COMPANY, INC.

"RED FLAG" RULES COMPLIANCE POLICY

Effective November 1, 2008, legislation for Section 114 of the Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), also known as the "Red Flag Rules," requires every creditor, including Castleberry Telephone Company, Inc. ("Castleberry"), to develop and implement a written Identity Theft Prevention Program ("Program") to detect, prevent and mitigate identity theft in connection with certain existing accounts or the opening of certain accounts. Section 114 also requires card issuers to develop reasonable policies and procedures regarding changes of address, and Section 315 requires users of consumer reports to implement policies and procedures needed to respond to address discrepancies.

Accounts Covered

The rules are applicable to certain new and existing accounts where an ongoing relationship exists between a subscriber and Castleberry, including personal accounts that involve or are designed to permit multiple payments or transactions, such as cell phone and wireline service accounts, for which there is a reasonably foreseeable risk to subscribers or Castleberry from identity theft. Single, non-continuing transactions, where no ongoing relationship exists between the subscriber and Castleberry, are not covered by the rules.

Program Provisions

Castleberry's Program identifies relevant patterns, practices and specific forms of activity that are "red flags" signaling possible identity theft. The final rules and guidelines do not require the use of any specific technology, systems, processes or methodology, nor is Castleberry required to develop duplicate policies and procedures when its existing processes control reasonably foreseeable risks to subscribers or Castleberry from identity theft.

Castleberry has instituted the following procedures in response to "red flags" from the following categories, including, as applicable, "red flags" derived from incidents of identity theft that Castleberry has experienced; methods of identity theft identified by Castleberry that reflect changes in identity theft risks; and supervisory guidance.

Recordkeeping

Although the FTC's rules do not provide guidelines regarding documentation of activities that implicate or trigger "red flags," Castleberry will follow standard procedures for documentation of any such activities and company responses, as directed by supervisory personnel, and maintain such records in accordance with Castleberry's record retention policies.

Alerts, Notifications or Warnings from a Consumer Reporting Agency

Castleberry does not request or receive reports, alerts, notifications or warnings from any consumer reporting agency that may indicate that a subscriber's identity could have been stolen or compromised. However, Castleberry will continue to follow the relevant rules and regulations of the Alabama Public Service Commission regarding the establishment of service for those customers who have had a utility account closed for nonpayment and/or abuse of service.

1. A fraud or active duty alert is included with a consumer report.

   Not applicable. Castleberry does not receive or check consumer reports.

2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.

   Not applicable. Castleberry does not receive or check consumer reports.

3. A consumer reporting agency provides a notice of address discrepancy.

   Not applicable. Castleberry does not receive or check consumer reports.

4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or subscriber, such as:

   a. A recent and significant increase in the volume of inquiries;

   b. An unusual number of recently established credit relationships; or

   c. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

   Not applicable. Castleberry does not receive or check consumer reports.

Suspicious Documents

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

   For applicants for new service,

   - Castleberry will follow established customer authentication procedures, requiring presentation of a government issued photo ID (preferably, driver's license),
   - make a copy of the suspicious ID,
   - request additional proof of identity and/or compare signatures among documents presented,
   - refuse to open an account until the discrepancy is resolved, and/or

- in its discretion, notify law enforcement or the agency purportedly issuing the suspicious document.

- **Under these circumstances, no new accounts will be opened without requiring the customer to come into the company's office and verifying his/her identity in person.**

For existing subscribers,

- Castleberry will follow established customer authentication procedures, requiring presentation of a government issued photo ID (preferably, driver's license) for subscribers making their requests in person,

- make a copy of the suspicious ID,

- request additional proof of identity and/or compare signatures among documents presented,

- ask for the account password,

- refuse to make changes to the account until the discrepancy is resolved,

- check account records for additional authorized persons,

- monitor the existing account for evidence of identity theft, and/or

- in its discretion, notify law enforcement or the agency purportedly issuing the suspicious document.

6. <u>The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification</u>.

For applicants for new service,

- Castleberry will follow established customer authentication procedures, requiring presentation of a government issued photo ID (preferably, driver's license),

- make a copy of the suspicious ID,

- request additional proof of identity that includes a photograph and/or physical description that matches the appearance of the applicant,

- refuse to open an account until the discrepancy is resolved, and/or

- in its discretion, notify law enforcement or the agency purportedly issuing the suspicious identification.

For existing subscriber accounts,

- Castleberry will follow established customer authentication procedures, requiring presentation of a government issued photo ID (preferably, driver's license) for subscribers making their requests in person,
- make a copy of the suspicious ID,
- request additional proof of identity that includes a photograph and/or physical description that matches the appearance of the applicant,
- ask for the account password,
- refuse to make changes to the account until the discrepancy is resolved,
- check account records for additional authorized persons,
- mail notice of the attempted changes to the account to the subscriber's address of record,
- monitor the existing account for evidence of identity theft, and/or
- in its discretion, notify law enforcement or the agency purportedly issuing the suspicious document.

7. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

For applicants for new service,

- Castleberry will follow established customer authentication procedures, requiring presentation of a government issued photo ID (preferably, driver's license),
- make a copy of the suspicious ID,
- request additional proof of identity that contains the same information found to be inconsistent in the identification presented,
- refuse to open an account until the discrepancy is resolved, and/or
- in its discretion, notify law enforcement of the suspicious information.

For existing subscriber accounts,

- Castleberry will follow established customer authentication procedures, requiring presentation of a government issued photo ID (preferably, driver's license) for subscribers making their requests in person,

- make a copy of the suspicious ID,
- request additional proof of identity that contains the same information found to be inconsistent in the identification presented,
- ask for the account password,
- refuse to make changes to the account until the discrepancy is resolved,
- check account records for additional authorized persons,
- mail notice of the attempted changes to the account to the subscriber's address of record,
- monitor the existing account for evidence of identity theft, and/or
- in its discretion, notify law enforcement of the suspicious information.

8. Other information on the identification is not consistent with readily accessible information that is on file with Castleberry, such as a signature card or a recent check.

- Castleberry will follow established customer authentication procedures, requiring presentation of a government issued photo ID (preferably, driver's license) for subscribers making their requests in person,
- make a copy of the suspicious ID,
- request additional proof of identity that contains the same information found to be inconsistent in the identification presented,
- ask for the account password,
- refuse to make changes to the account until the discrepancy is resolved,
- *follow CPNI rules regarding access to customer proprietary information,*
- check account records for additional authorized persons,
- mail notice of the attempted changes to the account to the subscriber's address of record,
- monitor the existing account for evidence of identity theft, and/or
- in its discretion, notify law enforcement of the suspicious information.

9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

For an application for a new customer account,

- Castleberry will follow established customer authentication procedures, requiring presentation of a government issued photo ID (preferably, driver's license) for subscribers making their requests in person,
- refuse to open an account at that time, and
- require a new application.

For an application to add or change services to an existing account,

- Castleberry will follow established customer authentication procedures, requiring presentation of a government issued photo ID (preferably, driver's license) for subscribers making their requests in person,
- ask for the account password,
- check account records for additional authorized persons,
- mail notice of the attempted changes to the account to the subscriber's address of record, and/or
- monitor the existing account for evidence of identity theft.

Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by Castleberry.

For example:

a. The address does not match any address in the consumer report; or

b. The Social Security Number ("SSN") has not been issued, or is listed on the Social Security Administration's Death Master File.

Castleberry does not utilize consumer reports, social security numbers or any other external sources to verify personal identifying information. Castleberry will continue to follow its established customer authentication procedures, requiring presentation of a government issued photo ID (preferably, driver's license) before initiating new services of any kind.

11. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the subscriber.

For an application for a new customer account,

- Castleberry will follow established customer authentication procedures, requiring presentation of a government issued photo ID (preferably, driver's license),
- make a copy of the suspicious documentation,
- request additional proof of identity that contains the same information found to be inconsistent in the identification presented, and/or
- refuse to open an account until the discrepancy is resolved.
- **Under these circumstances, no new accounts will be opened without requiring the customer to come into the company's office and verifying his/her identity in person.**

For an application to add or change services to an existing account,

- Castleberry will follow established customer authentication procedures, requiring presentation of a government issued photo ID (preferably, driver's license) for subscribers making their requests in person,
- make a copy of the suspicious documentation,
- ask for the account password,
- request additional proof of identity that contains the same information found to be inconsistent in the identification presented,
- check account records for additional authorized persons,
- refuse to make changes to the account until the discrepancy is resolved,
- *follow CPNI rules regarding access to customer proprietary information*,
- mail notice of the attempted changes to the account and possible fraudulent activity to the subscriber's address of record, including a referral to a reputable service providing assistance in resolving identity theft issues,
- monitor the existing account for evidence of identity theft.

12. <u>Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by Castleberry.</u>

For an application for a new customer account,

- Castleberry will follow established customer authentication procedures, requiring presentation of a government issued photo ID (preferably, driver's license) and social security number,

- make a copy of the suspicious ID,
- request additional proof of identity,
- refuse to open an account until the discrepancy is resolved, and/or
- in its discretion, notify law enforcement of the attempted activity.
- **Under these circumstances, no new accounts will be opened without requiring the customer to come into the company's office and verifying his/her identity in person.**

For an application to add or change services to an existing account,

- Castleberry will follow established customer authentication procedures, requiring presentation of a government issued photo ID (preferably, driver's license) for subscribers making their requests in person,
- ask for the account password,
- check account records for additional authorized persons,
- mail notice of the attempted changes to the account and possible fraudulent activity to the subscriber's address of record, and/or
- monitor the existing account for evidence of identity theft.

    a. <u>The address on an application is the same as the address provided on a fraudulent application</u>.

In addition, the address must be verified by Castleberry.

For existing customers with a discrepancy in address, Castleberry may verify the new address by:

- using the E-911 database,
- asking for additional proof of address change, including, but not limited to, presentation of other utility bills bearing the new address, newly issued driver's license or other government issued ID, paycheck stub or employer's verification of new address, and/or
- mailing notice of the account change to the subscriber's address of record.

For new applicants for service who have recently moved to the Castleberry service area, Castleberry may verify the new address by

- asking for additional proof of address change, including, but not limited to, presentation of other utility bills bearing the new address, newly issued driver's license or other government issued ID, paycheck stub or employer's verification of new address.

b. The phone number on an application is the same as the number provided on a fraudulent application.

Not applicable – telephone number is assigned by Castleberry itself.

Castleberry will follow its internal rules of customer authentication, especially if a specific phone number is requested.

In addition, for an application for a new customer account,

- Castleberry will follow established customer authentication procedures, requiring presentation of a government issued photo ID (preferably, driver's license),
- make a copy of the suspicious ID,
- request additional proof of identity, and/or
- refuse to open an account until the discrepancy is resolved.

For an application to add or change services to an existing account,

- Castleberry will follow established customer authentication procedures, requiring presentation of a government issued photo ID (preferably, driver's license) for subscribers making their requests in person,
- ask for the account password,
- check account records for additional authorized persons,
- mail notice of the attempted changes to the account and possible fraudulent activity to the subscriber's address of record, including a referral to a reputable service providing assistance in resolving identity theft issues, and/or
- monitor the existing account for evidence of identity theft.

13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by Castleberry.

Castleberry will refuse to open or change an account until the issue is resolved.

a. The address on an application is fictitious, a mail drop, or prison; or

In addition, the address must be verified by Castleberry.

For existing customers with a discrepancy in address, Castleberry may must first verify the identity of the subscriber by asking for the account password, if the request is made by telephone, and/or a photo ID, for subscribers presenting in person, and verify the new address by

- using the E-911 database,
- asking for additional proof of address change, including, but not limited to, presentation of other utility bills bearing the new address, newly issued driver's license or other government issued ID, paycheck stub or employer's verification of new address,
- check records for additional authorized persons on the account, and/or
- mailing notice of the account change and possible fraudulent activity to the subscriber's address of record to the subscriber's address of record.

For new applicants for service who have recently moved to the Castleberry service area, Castleberry may verify the new address by

- asking for additional proof of address change, including, but not limited to, presentation of other utility bills bearing the new address, newly issued driver's license or other government issued ID, paycheck stub or employer's verification of new address.

b. The phone number is invalid, or is associated with a pager or answering service.

Not applicable – telephone number is assigned by Castleberry itself.

Castleberry will follow its internal rules of customer authentication.

14. The SSN provided is the same as that submitted by other persons opening an account or other customers.

Not applicable. Castleberry does not utilize social security numbers in verifying the identity of any applicant of service.

15. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.

The address must be verified by Castleberry.

For existing customers with a discrepancy in address, Castleberry must first verify the identity of the subscriber by asking for the account password, if a request is made by

telephone, or a photo ID, for subscribers presenting in person, and may verify the new address by:

- using the E-911 database,
- asking for additional proof of address change, including, but not limited to, presentation of other utility bills bearing the new address, newly issued driver's license or other government issued ID, paycheck stub or employer's verification of new address,
- change passwords or PINS on existing account(s) affected,
- check records for additional authorized persons on the account, and/or
- mailing notice of the account change and possible fraudulent activity to the subscriber's address of record to the subscriber's address of record.

For new applicants for service who have recently moved to the Castleberry service area, Castleberry may verify the new address by

- asking for additional proof of address change, including, but not limited to, presentation of other utility bills bearing the new address, newly issued driver's license or other government issued ID, paycheck stub or employer's verification of new address.

16. The person opening the covered account or the subscriber fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

- Castleberry will refuse to open or change an account until information is provided and verified,
- ask for the account password from existing subscribers,
- change passwords or PINS on existing account(s) affected,
- check records for additional authorized persons on the account, and/or
- mail notice of the account change and possible fraudulent activity to the subscriber's address of record to the subscriber's address of record.

17. Personal identifying information provided is not consistent with personal identifying information that is on file with Castleberry.

- Castleberry will follow established customer authentication procedures, requiring presentation of a government issued photo ID (preferably, driver's license) for subscribers making their requests in person,

- make a copy of the suspicious ID,
- request additional proof of identity that contains the same information found to be inconsistent in the identification presented,
- ask for the account password,
- refuse to make changes to the account until the discrepancy is resolved,
- *follow CPNI rules regarding access to customer proprietary information,*
- check account records for additional authorized persons,
- mail notice of the attempted changes to the account to the subscriber's address of record,
- monitor the existing account for evidence of identity theft, and/or
- in its discretion, notify law enforcement of the suspicious information.

18. For creditors that use challenge questions, the person opening the covered account or the subscriber cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Not applicable. Castleberry does not use challenge questions, but will follow its internal rules of customer authentication, which require a password and a backup "secret question" known only to the subscriber or authorized persons on the account.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

19. Shortly following the notice of a change of address for a covered account, Castleberry receives a request for new, additional, or replacement cards or a cell phone, or for the addition of authorized users on the account.

Castleberry may not issue additional or replacement cards until it verifies the validity of the change of address, notifies the cardholder of the request and provides the cardholder with a reasonable means of promptly reporting incorrect address changes.

- Castleberry may verify the new address by using the E-911 database,
- ask for additional proof of address change, including, but not limited to, presentation of other utility bills bearing the new address, newly issued driver's license or other government issued ID, paycheck stub or employer's verification of new address,
- mail notice of the account changes and possible fraudulent activity to the subscriber's address of record, which has been associated with the account for thirty (30) days, and/or

- monitor account for evidence of identity theft.

Castleberry will also require a written request for additional authorized users on the account, signed by the subscriber of record, and check records for additional authorized persons on the account.

20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:

    a. The subscriber fails to make the first payment or makes an initial payment but no subsequent payments.

       Castleberry will follow the Alabama Public Service Commission's rules and its normal procedures for disconnection of service. Castleberry will ensure that the address of record for billing purposes is the same as that provided on the application for service.

21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example

    a. Nonpayment when there is no history of late or missed payments;

       - Castleberry will contact the customer by phone, if desired,
       - change passwords or PINS on existing account(s) affected, and/or
       - monitor the account for evidence of identity theft.

       Castleberry will follow the Alabama Public Service Commission's rules and its normal procedures for disconnection of service. Castleberry will ensure that the address of record for billing purposes is the same as that provided on the application for service.

    b. A material change in purchasing or spending patterns; or

       - Castleberry will require the associated password before adding any new services by telephone,
       - follow established customer authentication procedures, requiring presentation of a government issued photo ID (preferably, driver's license) for subscribers making their requests in person,
       - *follow CPNI rules regarding access to customer proprietary information,*
       - mail notice of account changes and possible fraudulent activity to the subscriber's address of record, which has been associated with the account for thirty (30) days,

- change passwords or PINS on existing account(s) affected,
- monitor accounts not subscribed to unlimited plans for spikes in long distance calling and place a block on the account until the subscriber has been contacted, and/or
- monitor the account for evidence of identity theft.

c. A material change in telephone call patterns in connection with a cellular phone account.

Castleberry does not offer cellular services, but will monitor affected accounts for additional evidence of identity theft.

22. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

Not applicable. Castleberry will follow the Alabama Public Service Commission's rules and its normal procedures for disconnection of service.

23. Mail sent to the subscriber is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the subscriber's covered account.

- Castleberry will require the established password before adding any new services by telephone,
- follow established customer authentication procedures, requiring presentation of a government issued photo ID (preferably, driver's license) for subscribers making their requests in person,
- contact the subscriber in person,
- mail notice of account changes and possible fraudulent activity to the subscriber's address of record, which has been associated with the account for thirty (30) days, including a referral to a reputable service providing assistance in resolving identity theft issues,
- change passwords or PINS on existing account(s) affected,
- close existing account and reopen with a new telephone number,
- follow address verification procedures for any new address provided by the subscriber and mail notice of that account change to the subscriber's address of record, which has been associated with the account for thirty (30) days, and/or
- monitor the account for evidence of identity theft.

24. Castleberry is notified that the subscriber is not receiving paper account statements.

- Castleberry will verify the address of record with the subscriber,
- follow address verification procedures for any new address provided by the subscriber, and/or
- monitor the account for evidence of identity theft.

Castleberry will follow the Alabama Public Service Commission's rules and its normal procedures for disconnection of service.

25. Castleberry is notified of unauthorized charges or transactions in connection with a subscriber's covered account.

- Castleberry will require the established password before adding any new services by telephone,
- follow established customer authentication procedures, requiring presentation of a government issued photo ID (preferably, driver's license) for subscribers making their requests in person,
- follow disputed charge procedures with the subscriber,
- check written requests for authorized users on the account, signed by the subscriber of record,
- mail notice of account changes and possible fraudulent activity to the subscriber's address of record, which has been associated with the account for thirty (30) days, including a referral to a reputable service providing assistance in resolving identity theft issues,
- change passwords or PINs on existing account(s) affected,
- close existing account and reopen with a new telephone number,
- follow address verification procedures for any new address provided by the subscriber and mail notice of that account change to the subscriber's address of record, which has been associated with the account for thirty (30) days, and/or
- monitor the account for evidence of identity theft.

Notice from Subscribers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts Held by Castleberry

26. Castleberry is notified by a subscriber, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

- Castleberry will contact the victim and require him/her to provide proof of identity for Castleberry's records,
- require the subscriber or victim to provide a written statement that he/she disputes the account,
- require the subscriber to provide proof of his/her identity, following established customer authentication procedures that require presentation of a government issued photo ID (preferably, driver's license) and social security number, and/or
- advise the subscriber or victim to notify law enforcement of the fraudulent activity,
- suspend the account if contact is not made with subscriber in a timely manner, and/or requested documentation is not provided in a timely manner, and/or
- close the account immediately if found to have been fraudulently established.

In addition, if the subscriber is the victim,

- change passwords or PINS on subscriber's existing account(s),
- close subscriber's existing account and reopen with a new telephone number, and/or
- monitor the account for evidence of identity theft.

27. Change of address request closely follows a request for new services or a material change in a customer's use of his/her service.

The address must be verified by Castleberry.

- Castleberry may verify the new address by using the E-911 database,
- ask for additional proof of address change, including, but not limited to, presentation of other utility bills bearing the new address, newly issued driver's license or other government issued ID, paycheck stub or employer's verification of new address,
- require the established password before adding any new services by telephone,

- follow established customer authentication procedures, requiring presentation of a government issued photo ID (preferably, driver's license) for subscribers making their requests in person,

- change passwords or PINS on existing account(s) affected,

- require a written request for additional authorized users on the account, signed by the subscriber of record and check records for additional authorized persons on the account,

- mail notice of the account changes and/or possible fraudulent activity to the subscriber's address of record, which has been associated with the account for thirty (30) days, and/or

- monitor account for evidence of identity theft.

28. Provide for periodic review and updates to Castleberry's red flag policies and procedures.

Castleberry's red flag policies and procedures will be reviewed once annually, with updates as required based on:

a. Castleberry's experiences with identity theft;

b. changes in methods of identity theft;

c. changes in methods to detect, prevent, and mitigate identity theft;

d. changes in the types of accounts that Castleberry offers or maintains; and

e. changes in Castleberry's business arrangements, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

29. The Program should have oversight by Castleberry's Board of Directors, an appropriate committee thereof, or in the absence of such a Board, a designated employee at the level of senior management.

Homer Holland will have responsibility of regulatory supervision over the Program.

30. The Board of Directors or a committee thereof must approve the initial written Program, but the rules provide Castleberry with the discretion to determine whether the Board or management will approve changes to the Program and the extent of Board involvement in the oversight, development, implementation and administration of the Program through:

Castleberry's initial program will be approved by Castleberry's Board of Directors; additional changes will require the approval of Homer Holland. The Board will have no involvement in the oversight, development, implementation and administration of the Program.

a. Assigning specific responsibility for the Program's implementation;

Homer Holland will be the individual responsible for the Program's simple mentation.

b. Reviewing annual reports prepared by staff regarding compliance by Castleberry, specifically addressing material matters related to the Program and evaluating issues such as: the effectiveness of Castleberry's policies and procedures in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for material changes to the Program;

Homer Holland will be the individual responsible for reviewing compliance reports, evaluating the effectiveness of Castleberry's program in addressing the risk of identity theft to Castleberry and its subscribers, evaluating service provider arrangements and company responses to incidents of identity theft, and recommending Program changes.

c. Approving material changes to the Program as necessary to address changing identity theft risks;

Homer Holland will be the individual responsible for approving material changes to the Program as necessary to address changing identity theft risks.

d. Training staff, as necessary, to effectively implement the Program; and

Homer Holland will be the individual responsible for training staff on an annual basis regarding the Program, content and implementation.

- Castleberry will set up training schedule,
- require employees to sign off on their receipt of the written policies and procedures, and their review and understanding of them, and
- document employees' participation in training and keep a copy of that document in Castleberry's personnel files.

e. Exercising appropriate and effective oversight of service providers engaged to perform an activity in connection with one or more covered accounts.

- Castleberry will ensure that any contracts with outside service providers contain a provision that the services are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft, and

- include a requirement by contract that the service provider have policies and procedures to detect relevant red flags that may arise in the performance of its activities, and to report the red flags to Castleberry or take appropriate steps to prevent or mitigate identity theft.