
**Columbus Eye Associates & Columbus Optical
Red Flags Rule Compliance Policy
Identity Theft Prevention and Detection Policies and Procedures**

It is the policy of Columbus Eye Associates & Columbus Optical to follow all federal and state laws and reporting requirements regarding identity theft. Specifically, this policy outlines how Columbus Eye Associates & Columbus Optical will (1) Identify Red Flags, (2) Detect Red Flags (3) Respond to Red Flags. A "Red Flag" as defined by this policy includes a pattern, practice, or specific account or record activity that indicates possible identity theft.

It is the policy of Columbus Eye Associates & Columbus Optical that this Identity theft prevention and detection and Red Flags Rule compliance policy is approved by the owners of Columbus Eye Associates & Columbus Optical as of May 1, 2009, and that the policy will be reviewed and approved annually.

It is the policy of Columbus Eye Associates & Columbus Optical that the Administrator of Columbus Eye Associates and Columbus Optical is assigned the responsibility of implementing and maintaining the Red Flags Rule requirements. Furthermore, it is the policy of this Columbus Eye Associates & Columbus Optical that this individual will be provided sufficient resources and authority to fulfill these responsibilities. At a minimum, it is the policy of Columbus Eye Associates & Columbus Optical that there will be one individual or job description designated as the privacy official.

It is the policy of Columbus Eye Associates & Columbus Optical that, pursuant to the existing HIPAA Security Rule, appropriate physical, administrative and technical safeguards will be in place to reasonably safeguard protected health information and sensitive information related to patient identity from any intentional or unintentional use or disclosure.

It is the policy of Columbus Eye Associates & Columbus Optical that its business associates must be contractually bound to protect sensitive patient information to the same degree as set forth in this policy. It is also the policy of Columbus Eye Associates & Columbus Optical that business associates who violate their agreement will be dealt with first by an attempt to correct the problem, and if that fails by termination of the agreement and discontinuation of services by the business associate.

It is the policy of Columbus Eye Associates & Columbus Optical that all members of its workforce will have informed and trained by the May 1, 2009 compliance date on the policies and procedures governing compliance with the Red Flags Rule. It is also the policy of Columbus Eye Associates & Columbus Optical that new staff of its workforce will receive training on these matters within a reasonable time after they have joined the workforce.

Columbus Office

100 Sweetbriar Drive
Columbus, Texas 78934
979-732-5771 – Telephone
979-732-6922 – Fax
800-460-EYES (3937) - Toll Free

Katy Office

21720 Kingsland Blvd., Suite 305
Katy, Texas 77450
281-829-EYES (3937) – Telephone
281-829-0599 – Fax

La Grange Office

108 N. Washington
La Grange, Texas 78945
979-968-3953 – Telephone
979-968-3435 – Fax

Sealy Office

2879 Hwy 36 South
Sealy, Texas 77474
979-885-0665 - Telephone
979-885-4110 – Fax

It is the policy of Columbus Eye Associates & Columbus Optical to provide training should any policy or procedure related to the Red Flags Rule materially change. This training will be provided within a reasonable time after the policy or procedure materially changes. Furthermore, it is the policy of Columbus Eye Associates & Columbus Optical that training will be documented, indicating participants, date and subject matter.

PROCEDURES

1. IDENTIFY RED FLAGS

In the course of caring for patients, Columbus Eye Associates & Columbus Optical may encounter inconsistent or suspicious documents, information or activity that may signal identity theft. Columbus Eye Associates & Columbus Optical identifies the following as potential Red Flags, and this policy includes procedures describing how to detect and respond to these Red Flags below:

- a. A complaint or question from a patient based on the patient's receipt of:
 - A bill for another individual;
 - A bill for a product or service that the patient denies receiving;
 - A bill from a health care provider that the patient never patronized; or
 - A notice of insurance benefits (or explanation of benefits) for health care services never received.
- b. Records showing medical treatment that is inconsistent with a physical examination or with a medical history as reported by the patient.
- c. A complaint or question from a patient about the receipt of a collection notice from a bill collector.
- d. A patient or health insurer report that coverage for legitimate hospital stays is denied because insurance benefits have been depleted or a lifetime cap has been reached.
- e. A complaint or question from a patient about information added to a credit report by a health care provider or health insurer.
- f. A dispute of a bill by a patient who claims to be the victim of any type of identity theft.
- g. A patient who has an insurance number but never produces an insurance card or other physical documentation of insurance.
- h. A notice or inquiry from an insurance fraud investigator for a private health insurer or a law enforcement agency, including but not limited to a Medicare or Medicaid fraud alert.

2. DETECT RED FLAGS

Columbus Eye Associates & Columbus Optical practice staff will be alert for discrepancies in documents and patient information that suggest risk of identity theft or fraud. Columbus Eye

Columbus Office

100 Sweetbriar Drive
Columbus, Texas 78934
979-732-5771 – Telephone
979-732-6922 – Fax
800-460-EYES (3937) - Toll Free

Katy Office

21720 Kingsland Blvd., Suite 305
Katy, Texas 77450
281-829-EYES (3937) – Telephone
281-829-0599 – Fax

La Grange Office

108 N. Washington
La Grange, Texas 78945
979-968-3953 – Telephone
979-968-3435 – Fax

Sealy Office

2879 Hwy 36 South
Sealy, Texas 77474
979-885-0665 - Telephone
979-885-4110 – Fax

Associates & Columbus Optical will verify patient identity, address and insurance coverage at the time of patient registration/check-in by doing the following:

- a. When a patient calls to request an appointment, the patient will be asked to bring the following at the time of the appointment:
 - Driver's license or other photo ID;
 - Current health insurance card; and
 - Utility bills or other correspondence showing current residence if the photo ID does not show the patient's current address. If the patient is a minor, the patient's parent or guardian should bring the information listed above.
- b. When the patient arrives for the appointment, the patient will be asked to produce the information listed above. This requirement may be waived for patients who have visited the practice within the last six months.
- c. If the patient has not completed the registration form within the last six months, registration staff will verify current information on file and, if appropriate, update the information.
- d. Staff will be alert for the possibility of identity theft in the following situations:
 - The photograph on a driver's license or other photo ID submitted by the patient does not resemble the patient.
 - The patient submits a driver's license, insurance card, or other identifying information that appears to be altered or forged.
 - Information on one form of identification the patient submitted is inconsistent with information on another form of identification or with information already in the practice's records.
 - An address or telephone number is discovered to be incorrect, non-existent or fictitious.
 - The patient fails to provide identifying information or documents.
 - The patient's signature does not match a signature in the practice's records.
 - The Social Security number or other identifying information the patient provided is the same as identifying information in the practice's records provided by another individual, or the Social Security number is invalid.

3. RESPOND TO RED FLAGS

If an employee of Columbus Eye Associates & Columbus Optical detects fraudulent activity or if a patient claims to be a victim of identity theft, Columbus Eye Associates & Columbus Optical will respond to and investigate the situation. If the fraudulent activity involves protected health information (PHI) covered under the HIPAA security standards, Columbus Eye Associates & Columbus Optical will also apply its existing HIPAA security policies and procedures to the response. If potentially fraudulent activity (a Red Flag) is detected by an employee of Columbus Eye Associates and Columbus Optical the following will occur:

Columbus Office

100 Sweetbriar Drive
Columbus, Texas 78934
979-732-5771 – Telephone
979-732-6922 – Fax
800-460-EYES (3937) - Toll Free

Katy Office

21720 Kingsland Blvd., Suite 305
Katy, Texas 77450
281-829-EYES (3937) – Telephone
281-829-0599 – Fax

La Grange Office

108 N. Washington
La Grange, Texas 78945
979-968-3953 – Telephone
979-968-3435 – Fax

Sealy Office

2879 Hwy 36 South
Sealy, Texas 77474
979-885-0665 - Telephone
979-885-4110 – Fax

- a. The employee will gather all documentation and report the incident to the Columbus Eye Associates and Columbus Optical Administrator.
- b. The Columbus Eye Associates and Columbus Optical Administrator will determine whether the activity is fraudulent or authentic.
- c. If the activity is determined to be fraudulent, then Columbus Eye Associates and Columbus Optical will take immediate action. Actions may include:
 - Cancel the transaction;
 - Notify appropriate law enforcement;
 - Notify the affected patient;
 - Notify affected physician(s); and
 - Assess impact to practice.
- e. If a patient claims to be a victim of identity theft:
 1. The patient should be encouraged to file a police report for identity theft if he/she has not done so already.
 2. The patient should be encouraged to complete the ID Theft Affidavit developed by the FTC, along with supporting documentation.
 3. Columbus Eye Associates & Columbus Optical will compare the patient's documentation with personal information in the practice's records.
 4. If following an investigation, it appears that the patient has been a victim of identity theft, Columbus Eye Associates and Columbus Optical will promptly consider what further remedial act/notifications may be needed under the circumstances.
 5. The physician will review the affected patient's medical record to confirm whether documentation was made in the patient's medical record that resulted in inaccurate information in the record. If inaccuracies due to identity theft exist, a notation should be made in the record to indicate identity theft.
 6. The practice medical records staff will determine whether any other records and/or ancillary service providers are linked to inaccurate information. Any additional files containing information relevant to identity theft will be removed and appropriate action taken. The patient is responsible for contacting ancillary service providers.
 7. If following an investigation it does not appear that the patient has been a victim of identity theft, Columbus Eye Associates and Columbus Optical will take whatever action it deems appropriate.

Columbus Office

100 Sweetbriar Drive
Columbus, Texas 78934
979-732-5771 – Telephone
979-732-6922 – Fax
800-460-EYES (3937) - Toll Free

Katy Office

21720 Kingsland Blvd., Suite 305
Katy, Texas 77450
281-829-EYES (3937) – Telephone
281-829-0599 – Fax

La Grange Office

108 N. Washington
La Grange, Texas 78945
979-968-3953 – Telephone
979-968-3435 – Fax

Sealy Office

2879 Hwy 36 South
Sealy, Texas 77474
979-885-0665 - Telephone
979-885-4110 – Fax

[Code of Federal Regulations]
[Title 16, Volume 1]
[Revised as of January 1, 2008]
From the U.S. Government Printing Office via GPO Access
[CITE: 16CFR681 App A]

[Page 615-618]

TITLE 16--COMMERCIAL PRACTICES

CHAPTER I--FEDERAL TRADE COMMISSION

PART 681_IDENTITY THEFT RULES--Table of Contents

Sec. Appendix A to Part 681--Interagency Guidelines on Identity Theft
Detection, Prevention, and Mitigation

Section 681.2 of this part requires each financial institution and creditor that offers or maintains one or more covered accounts, as defined in Sec. 681.2(b)(3) of this part, to develop and provide for the continued administration of a written Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. These guidelines are intended to assist financial institutions and creditors in the formulation and maintenance of a Program that satisfies the requirements of Sec. 681.2 of this part.

[[Page 616]]

I. The Program

In designing its Program, a financial institution or creditor may incorporate, as appropriate, its existing policies, procedures, and other arrangements that control reasonably foreseeable risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.

II. Identifying Relevant Red Flags

(a) Risk Factors. A financial institution or creditor should consider the following factors in identifying relevant Red Flags for covered accounts, as appropriate:

- (1) The types of covered accounts it offers or maintains;
- (2) The methods it provides to open its covered accounts;
- (3) The methods it provides to access its covered accounts; and
- (4) Its previous experiences with identity theft.

Columbus Office

100 Sweetbriar Drive
Columbus, Texas 78934
979-732-5771 – Telephone
979-732-6922 – Fax
800-460-EYES (3937) - Toll Free

Katy Office

21720 Kingsland Blvd., Suite 305
Katy, Texas 77450
281-829-EYES (3937) – Telephone
281-829-0599 – Fax

La Grange Office

108 N. Washington
La Grange, Texas 78945
979-968-3953 – Telephone
979-968-3435 – Fax

Sealy Office

2879 Hwy 36 South
Sealy, Texas 77474
979-885-0665 - Telephone
979-885-4110 – Fax

(b) Sources of Red Flags. Financial institutions and creditors should incorporate relevant Red Flags from sources such as:

- (1) Incidents of identity theft that the financial institution or creditor has experienced;
- (2) Methods of identity theft that the financial institution or creditor has identified that reflect changes in identity theft risks; and
- (3) Applicable supervisory guidance.

(c) Categories of Red Flags. The Program should include relevant Red Flags from the following categories, as appropriate. Examples of Red Flags from each of these categories are appended as supplement A to this appendix A.

- (1) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
- (2) The presentation of suspicious documents;
- (3) The presentation of suspicious personal identifying information, such as a suspicious address change;
- (4) The unusual use of, or other suspicious activity related to, a covered account; and
- (5) Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.

III. Detecting Red Flags

The Program's policies and procedures should address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts, such as by:

- (a) Obtaining identifying information about, and verifying the identity of, a person opening a covered account, for example, using the policies and procedures regarding identification and verification set forth in the Customer Identification Program rules implementing 31 U.S.C. 5318(l) (31 CFR 103.121); and
- (b) Authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.

IV. Preventing and Mitigating Identity Theft

The Program's policies and procedures should provide for appropriate responses to the Red Flags the financial institution or creditor has detected that are commensurate with the degree of risk posed. In determining an appropriate response, a financial institution or creditor should consider aggravating factors that may heighten the risk of

Columbus Office

100 Sweetbriar Drive
Columbus, Texas 78934
979-732-5771 – Telephone
979-732-6922 – Fax
800-460-EYES (3937) - Toll Free

Katy Office

21720 Kingsland Blvd., Suite 305
Katy, Texas 77450
281-829-EYES (3937) – Telephone
281-829-0599 – Fax

La Grange Office

108 N. Washington
La Grange, Texas 78945
979-968-3953 – Telephone
979-968-3435 – Fax

Sealy Office

2879 Hwy 36 South
Sealy, Texas 77474
979-885-0665 - Telephone
979-885-4110 – Fax

identity theft, such as a data security incident that results in unauthorized access to a customer's account records held by the financial institution, creditor, or third party, or notice that a customer has provided information related to a covered account held by the financial institution or creditor to someone fraudulently claiming to represent the financial institution or creditor or to a fraudulent website. Appropriate responses may include the following:

- (a) Monitoring a covered account for evidence of identity theft;
- (b) Contacting the customer;
- (c) Changing any passwords, security codes, or other security devices that permit access to a covered account;
- (d) Reopening a covered account with a new account number;
- (e) Not opening a new covered account;
- (f) Closing an existing covered account;
- (g) Not attempting to collect on a covered account or not selling a covered account to a debt collector;
- (h) Notifying law enforcement; or
- (i) Determining that no response is warranted under the particular circumstances.

V. Updating the Program

Financial institutions and creditors should update the Program (including the Red Flags determined to be relevant) periodically, to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft, based on factors such as:

- (a) The experiences of the financial institution or creditor 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 the financial institution or creditor offers or maintains; and
- (e) Changes in the business arrangements of the financial institution or creditor, including mergers, acquisitions, alliances,

[[Page 617]]

joint ventures, and service provider arrangements.

VI. Methods for Administering the Program

(a) Oversight of Program. Oversight by the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management should include:

(1) Assigning specific responsibility for the Program's implementation;

(2) Reviewing reports prepared by staff regarding compliance by the financial institution or creditor with Sec. 681.2 of this part; and

(3) Approving material changes to the Program as necessary to address changing identity theft risks.

(b) Reports. (1) In general. Staff of the financial institution or creditor responsible for development, implementation, and administration of its Program should report to the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management, at least annually, on compliance by the financial institution or creditor with Sec. 681.2 of this part.

(2) Contents of report. The report should address material matters related to the Program and evaluate issues such as: The effectiveness of the policies and procedures of the financial institution or creditor 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.

(c) Oversight of service provider arrangements. Whenever a financial institution or creditor engages a service provider to perform an activity in connection with one or more covered accounts the financial institution or creditor should take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. For example, a financial institution or creditor could require the service provider by contract to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either report the Red Flags to the financial institution or creditor, or to take appropriate steps to prevent or mitigate identity theft.

VII. Other Applicable Legal Requirements

Financial institutions and creditors should be mindful of other related legal requirements that may be applicable, such as:

(a) For financial institutions and creditors that are subject to 31 U.S.C. 5318(g), filing a Suspicious Activity Report in accordance with applicable law and regulation;

(b) Implementing any requirements under 15 U.S.C. 1681c-1(h) regarding the circumstances under which credit may be extended when the financial institution or creditor detects a fraud or active duty alert;

(c) Implementing any requirements for furnishers of information to consumer reporting agencies under 15 U.S.C. 1681s-2, for example, to correct or update inaccurate or incomplete information, and to not

Columbus Office

100 Sweetbriar Drive
Columbus, Texas 78934
979-732-5771 – Telephone
979-732-6922 – Fax
800-460-EYES (3937) - Toll Free

Katy Office

21720 Kingsland Blvd., Suite 305
Katy, Texas 77450
281-829-EYES (3937) – Telephone
281-829-0599 – Fax

La Grange Office

108 N. Washington
La Grange, Texas 78945
979-968-3953 – Telephone
979-968-3435 – Fax

Sealy Office

2879 Hwy 36 South
Sealy, Texas 77474
979-885-0665 – Telephone
979-885-4110 – Fax

report information that the furnisher has reasonable cause to believe is inaccurate; and

(d) Complying with the prohibitions in 15 U.S.C. 1681m on the sale, transfer, and placement for collection of certain debts resulting from identity theft.

Supplement A to Appendix A

In addition to incorporating Red Flags from the sources recommended in section II.b. of the Guidelines in Appendix A of this part, each financial institution or creditor may consider incorporating into its Program, whether singly or in combination, Red Flags from the following illustrative examples in connection with covered accounts:

Alerts, Notifications or Warnings from a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer report.
2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
3. A consumer reporting agency provides a notice of address discrepancy, as defined in Sec. 681.1(b) of this part.
4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
 - a. A recent and significant increase in the volume of inquiries;
 - b. An unusual number of recently established credit relationships;
 - c. A material change in the use of credit, especially with respect to recently established credit relationships; or
 - d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious Documents

5. Documents provided for identification appear to have been altered or forged.
6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
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.
8. Other information on the identification is not consistent with readily accessible information that is on file with the financial

[[Page 618]]

Columbus Office

100 Sweetbriar Drive
Columbus, Texas 78934
979-732-5771 – Telephone
979-732-6922 – Fax
800-460-EYES (3937) - Toll Free

Katy Office

21720 Kingsland Blvd., Suite 305
Katy, Texas 77450
281-829-EYES (3937) – Telephone
281-829-0599 – Fax

La Grange Office

108 N. Washington
La Grange, Texas 78945
979-968-3953 – Telephone
979-968-3435 – Fax

Sealy Office

2879 Hwy 36 South
Sealy, Texas 77474
979-885-0665 - Telephone
979-885-4110 – Fax

institution or creditor, such as a signature card or a recent check.

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

Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. 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.

11. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.

12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

- a. The address on an application is the same as the address provided on a fraudulent application; or
- b. The phone number on an application is the same as the number provided on a fraudulent application.

13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

- a. The address on an application is fictitious, a mail drop, or a prison; or
- b. The phone number is invalid, or is associated with a pager or answering service.

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

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.

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

17. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.

18. For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be

Columbus Office

100 Sweetbriar Drive
Columbus, Texas 78934
979-732-5771 – Telephone
979-732-6922 – Fax
800-460-EYES (3937) - Toll Free

Katy Office

21720 Kingsland Blvd., Suite 305
Katy, Texas 77450
281-829-EYES (3937) – Telephone
281-829-0599 – Fax

La Grange Office

108 N. Washington
La Grange, Texas 78945
979-968-3953 – Telephone
979-968-3435 – Fax

Sealy Office

2879 Hwy 36 South
Sealy, Texas 77474
979-885-0665 - Telephone
979-885-4110 – Fax

available from a wallet or consumer report.

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, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users 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 majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or

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

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;

b. A material increase in the use of available credit;

c. A material change in purchasing or spending patterns;

d. A material change in electronic fund transfer patterns in connection with a deposit account; or

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

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).

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

24. The financial institution or creditor is notified that the customer is not receiving paper account statements.

25. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.

Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Covered Accounts Held by the Financial Institution or Creditor

26. The financial institution or creditor is notified by a customer, 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.

Columbus Office

100 Sweetbriar Drive
Columbus, Texas 78934
979-732-5771 – Telephone
979-732-6922 – Fax
800-460-EYES (3937) - Toll Free

Katy Office

21720 Kingsland Blvd., Suite 305
Katy, Texas 77450
281-829-EYES (3937) – Telephone
281-829-0599 – Fax

La Grange Office

108 N. Washington
La Grange, Texas 78945
979-968-3953 – Telephone
979-968-3435 – Fax

Sealy Office

2879 Hwy 36 South
Sealy, Texas 77474
979-885-0665 – Telephone
979-885-4110 – Fax

Documentation of Good Faith Effort

1. DETECT RED FLAGS

Columbus Eye Associates & Columbus Optical practice staff will be alert for discrepancies in documents and patient information that suggest risk of identity theft or fraud. Columbus Eye Associates & Columbus Optical will verify patient identity, address and insurance coverage at the time of patient registration/check-in by doing the following:

- a. When a patient calls to request an appointment, the patient will be asked to bring the following at the time of the appointment:
 - Driver's license or other photo ID;
 - Current health insurance card; and
 - Utility bills or other correspondence showing current residence if the photo ID does not show the patient's current address. If the patient is a minor, the patient's parent or guardian should bring the information listed above.
- b. When the patient arrives for the appointment, the patient will be asked to produce the information listed above. This requirement may be waived for patients who have visited the practice within the last six months.
- c. If the patient has not completed the registration form within the last six months, registration staff will verify current information on file and, if appropriate, update the information.
- d. Staff will be alert for the possibility of identity theft in the following situations:
 - The photograph on a driver's license or other photo ID submitted by the patient does not resemble the patient.
 - The patient submits a driver's license, insurance card, or other identifying information that appears to be altered or forged.
 - Information on one form of identification the patient submitted is inconsistent with information on another form of identification or with information already in the practice's records.
 - An address or telephone number is discovered to be incorrect, non-existent or fictitious.
 - The patient fails to provide identifying information or documents.
 - The patient's signature does not match a signature in the practice's records.
 - The Social Security number or other identifying information the patient provided is the same as identifying information in the practice's records provided by another individual, or the Social Security number is invalid.

On this date _____ the person listed below did not provide appropriate documentation to Columbus Eye Associates and Columbus Optical staff so that their identity could be verified with the information that we have on record. A good faith effort was made to obtain and verify the identity of the person listed below; however, proper identification was not verified because:

Name of Person Who Presented: _____

Patient Account Trying To Verify: _____

Patient Medical Record Trying To Verify: _____

Person did not provide an appropriate photo ID with information on it that matched what we have on file.

Patient was unable to sign or initial because: _____

The patient had a medical emergency, and an attempt to obtain an appropriate photo ID with information on it that matched what we have on file will be made at the next available opportunity.

Other reason (describe): _____

Name of Employee Completing Form

Signature of Employee Completing Form



Quality Eye Care Since 1953



Fashionable Eye Wear Since 1960

**Red Flags Rule Compliance Policy
Identity Theft Prevention and Detection Policies and Procedures**

I acknowledge that I received, read, understand and agree to comply with the Columbus Eye Associates and Columbus Optical Red Flags Rule Compliance Policy and Identity Theft Prevention and Detection Policies and Procedures. I acknowledge that by reading and having the Administrator of Columbus Eye Associates and Columbus Optical available for any questions that I might have I have received the appropriate training to follow the policies and procedures created in these documents to identify, detect, and prevent identity theft for our patients.

Employee Name

Employee Signature

Date

Columbus Office

100 Sweetbriar Drive
Columbus, Texas 78934
979-732-5771 – Telephone
979-732-6922 – Fax
800-460-EYES (3937) - Toll Free

Katy Office

21720 Kingsland Blvd., Suite 305
Katy, Texas 77450
281-829-EYES (3937) – Telephone
281-829-0599 – Fax

La Grange Office

108 N. Washington
La Grange, Texas 78945
979-968-3953 – Telephone
979-968-3435 – Fax

Sealy Office

2879 Hwy 36 South
Sealy, Texas 77474
979-885-0665 - Telephone
979-885-4110 – Fax

INSTRUCTIONS FOR COMPLETING THE ID THEFT AFFIDAVIT

To make certain that you do not become responsible for any debts incurred by an identity thief, you must prove to each of the companies where accounts were opened in your name that you didn't create the debt. The ID Theft Affidavit was developed by a group of credit grantors, consumer advocates, and attorneys at the Federal Trade Commission (FTC) for this purpose. Importantly, this affidavit is only for use where a new account was opened in your name. If someone made unauthorized charges to an existing account, call the company for instructions.

While many companies accept this affidavit, others require that you submit more or different forms. Before you send the affidavit, contact each company to find out if they accept it. If they do not accept the ID Theft Affidavit, ask them what information and/or documentation they require.

You may not need the ID Theft Affidavit to absolve you of debt resulting from identity theft if you obtain an Identity Theft Report. We suggest you consider obtaining an Identity Theft Report where a new account was opened in your name. An Identity Theft Report can be used to (1) permanently block fraudulent information from appearing on your credit report; (2) ensure that debts do not reappear on your credit reports; (3) prevent a company from continuing to collect debts or selling the debt to others for collection; and (4) obtain an extended fraud alert.

The ID Theft Affidavit may be required by a company in order for you to obtain applications or other transaction records related to the theft of your identity. These records may help you prove that you are a victim. For example, you may be able to show that the signature on an application is not yours. These documents also may contain information about the identity thief that is valuable to law enforcement.

This affidavit has two parts:

- Part One — the ID Theft Affidavit — is where you report general information about yourself and the theft.
- Part Two — the Fraudulent Account Statement — is where you describe the fraudulent account(s) opened in your name. Use a separate Fraudulent Account Statement for each company you need to write to.

When you send the affidavit to the companies, attach copies (NOT originals) of any supporting documents (for example, driver's license or police report). Before submitting your affidavit, review the disputed account(s) with family members or friends who may have information about the account(s) or access to them.

Complete this affidavit as soon as possible. Many creditors ask that you send it within two weeks. Delays on your part could slow the investigation.

Be as accurate and complete as possible. You may choose not to provide some of the information requested. However, incorrect or incomplete information will slow the process of investigating your claim and absolving the debt. Print clearly.

When you have finished completing the affidavit, mail a copy to each creditor, bank, or company that provided the thief with the unauthorized credit, goods, or services you describe. Attach a copy of the Fraudulent Account Statement with information only on accounts opened at the institution to which you are sending the packet, as well as any other supporting documentation you are able to provide.

Send the appropriate documents to each company by certified mail, return receipt requested, so you can prove that it was received. The companies will review your claim and send you a written response telling you the outcome of their investigation. Keep a copy of everything you submit.

If you are unable to complete the affidavit, a legal guardian or someone with power of attorney may complete it for you. Except as noted, the information you provide will be used only by the company to process your affidavit, investigate the events you report, and help stop further fraud. If this affidavit is requested in a lawsuit, the company might have to provide it to the requesting party. Completing this affidavit does not guarantee that the identity thief will be prosecuted or that the debt will be cleared.

If you haven't already done so, report the fraud to the following organizations:

1. Any one of the nationwide consumer reporting companies to place a fraud alert on your credit report. Fraud alerts can help prevent an identity thief from opening any more accounts in your name. The company you call is required to contact the other two, which will place an alert on their versions of your report, too.

- **Equifax:** 1-800-525-6285; www.equifax.com
- **Experian:** 1-888-EXPERIAN (397-3742); www.experian.com
- **TransUnion:** 1-800-680-7289; www.transunion.com

In addition, once you have placed a fraud alert, you're entitled to order one free credit report from each of the three consumer reporting companies, and, if you ask, they will display only the last four digits of your Social Security number on your credit reports.

2. The security or fraud department of each company where you know, or believe, accounts have been tampered with or opened fraudulently. Close the accounts. Follow up in writing, and include copies (NOT originals) of supporting documents. **It's important to notify credit card companies and banks in writing.** Send your letters by certified mail, return receipt requested, so you can document what the company received and when. Keep a file of your correspondence and enclosures.

When you open new accounts, use new Personal Identification Numbers (PINs) and passwords. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your Social Security number, your phone number, or a series of consecutive numbers.

3. Your local police or the police in the community where the identity theft took place. Provide a copy of your ID Theft Complaint filed with the FTC (see below), to be incorporated into the police report. Get a copy of the police report or, at the very least, the number of the report. It can help you deal with creditors who need proof of the crime. If the police are reluctant to take your report, ask to file a "Miscellaneous Incidents" report, or try another jurisdiction, like your state police. You also can check with your state Attorney General's office to find out if state law requires the police to take reports for identity theft. Check the Blue Pages of your telephone directory for the phone number or check www.naag.org for a list of state Attorneys General.
4. The Federal Trade Commission. By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials across the nation track down identity thieves and stop them. The FTC also can refer victims' complaints to other government agencies and companies for further action, as well as investigate companies for violations of laws that the FTC enforces.

You can file a complaint online at www.consumer.gov/idtheft. If you don't have Internet access, call the FTC's Identity Theft Hotline, toll-free: 1-877-IDTHEFT (438-4338); TTY: 1-866-653-4261; or write: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. When you file an ID Theft Complaint with the FTC online, you will be given the option to print a copy of your ID Theft Complaint. You should bring a copy of the printed ID Theft Complaint with you to the police to be incorporated into your police report. The ID Theft Complaint, in conjunction with the police report, can create an Identity Theft Report that will help you recover more quickly. The ID Theft Complaint provides the supporting details necessary for an Identity Theft Report, which go beyond the details of a typical police report.

**DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER
GOVERNMENT AGENCY**

ID Theft Affidavit

Victim Information

- (1) My full legal name is _____
(First) (Middle) (Last) (Jr., Sr., III)
- (2) (If different from above) When the events described in this affidavit took place, I was known as

(First) (Middle) (Last) (Jr., Sr., III)
- (3) My date of birth is _____
(day/month/year)
- (4) My Social Security number is _____
- (5) My driver's license or identification card state and number are _____
- (6) My current address is _____
City _____ State _____ Zip Code _____
- (7) I have lived at this address since _____
(month/year)
- (8) (If different from above) When the events described in this affidavit took place, my address was

City _____ State _____ Zip Code _____
- (9) I lived at the address in Item 8 from _____ until _____
(month/year) (month/year)
- (10) My daytime telephone number is (_____) _____
My evening telephone number is (_____) _____

**DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER
GOVERNMENT AGENCY**

How the Fraud Occurred

Check all that apply for items 11 - 17:

- (11) I did not authorize anyone to use my name or personal information to seek the money, credit, loans, goods or services described in this report.
- (12) I did not receive any benefit, money, goods or services as a result of the events described in this report.
- (13) My identification documents (for example, credit cards; birth certificate; driver’s license; Social Security card; etc.) were stolen lost on or about _____ (day/month/year).
- (14) To the best of my knowledge and belief, the following person(s) used my information (for example, my name, address, date of birth, existing account numbers, Social Security number, mother’s maiden name, etc.) or identification documents to get money, credit, loans, goods or services without my knowledge or authorization:

Name (if known)

Name (if known)

Address (if known)

Address (if known)

Phone number(s) (if known)

Phone number(s) (if known)

Additional information (if known)

Additional information (if known)

- (15) I do NOT know who used my information or identification documents to get money, credit, loans, goods or services without my knowledge or authorization.

- (16) Additional comments: (For example, description of the fraud, which documents or information were used or how the identity thief gained access to your information.)

(Attach additional pages as necessary.)

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY

Victim's Law Enforcement Actions

- (17) (check one) I am am not willing to assist in the prosecution of the person(s) who committed this fraud.
- (18) (check one) I am am not authorizing the release of this information to law enforcement for the purpose of assisting them in the investigation and prosecution of the person(s) who committed this fraud.
- (19) (check all that apply) I have have not reported the events described in this affidavit to the police or other law enforcement agency. The police did did not write a report. In the event you have contacted the police or other law enforcement agency, please complete the following:

(Agency #1)

(Date of report)

(Phone number)

(Officer/Agency personnel taking report)

(Report number, if any)

(email address, if any)

(Agency #2)

(Date of report)

(Phone number)

(Officer/Agency personnel taking report)

(Report number, if any)

(email address, if any)

Documentation Checklist

Please indicate the supporting documentation you are able to provide to the companies you plan to notify. Attach copies (NOT originals) to the affidavit before sending it to the companies.

- (20) A copy of a valid government-issued photo-identification card (for example, your driver's license, state-issued ID card or your passport). If you are under 16 and don't have a photo-ID, you may submit a copy of your birth certificate or a copy of your official school records showing your enrollment and place of residence.
- (21) Proof of residency during the time the disputed bill occurred, the loan was made or the other event took place (for example, a rental/lease agreement in your name, a copy of a utility bill or a copy of an insurance bill).

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY

- (22) A copy of the report you filed with the police or sheriff's department. If you are unable to obtain a report or report number from the police, please indicate that in Item 19. Some companies only need the report number, not a copy of the report. You may want to check with each company.

Signature

I certify that, to the best of my knowledge and belief, all the information on and attached to this affidavit is true, correct, and complete and made in good faith. I also understand that this affidavit or the information it contains may be made available to federal, state, and/or local law enforcement agencies for such action within their jurisdiction as they deem appropriate. I understand that knowingly making any false or fraudulent statement or representation to the government may constitute a violation of 18 U.S.C. § 1001 or other federal, state, or local criminal statutes, and may result in imposition of a fine or imprisonment or both.

(signature)

(date signed)

(Notary)

[Check with each company. Creditors sometimes require notarization. If they do not, please have one witness (non-relative) sign below that you completed and signed this affidavit.]

Witness:

(signature)

(printed name)

(date)

(telephone number)

**DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER
GOVERNMENT AGENCY**

Fraudulent Account Statement

Completing this Statement

- Make as many copies of this page as you need. **Complete a separate page for each company you're notifying and only send it to that company.** Include a copy of your signed affidavit.
- List only the account(s) you're disputing with the company receiving this form. **See the example below.**
- If a collection agency sent you a statement, letter or notice about the fraudulent account, attach a copy of that document (**NOT** the original).

I declare (check all that apply):

- As a result of the event(s) described in the ID Theft Affidavit, the following account(s) was/were opened at your company in my name without my knowledge, permission or authorization using my personal information or identifying documents:

Creditor Name/Address (the company that opened the account or provided the goods or services)	Account Number	Type of unauthorized credit/goods/services provided by creditor (if known)	Date issued or opened (if known)	Amount/Value provided (the amount charged or the cost of the goods/services)
Example Example National Bank 22 Main Street Columbus, Ohio 22722	01234567-89	auto loan	01/05/2002	\$25,500.00

- During the time of the accounts described above, I had the following account open with your company:

Billing name _____

Billing address _____

Account number _____

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER
GOVERNMENT AGENCY