

Excerpted from the Oklahoma Bar Journal, Vol. 80, No. 7, March 14, 2009, published by the Oklahoma Bar Association. Reprinted with permission.

Identity Theft Red Flags and Address Discrepancies

By Eric L. Johnson

Identity thieves use people's private and personally identifiable information to open new accounts and misuse existing accounts, creating havoc for consumers and businesses. The crime of identity theft afflicts millions of Americans each year, and in some cases, causes devastating damage to its victims. A recent Federal Trade Commission (FTC) report estimated that over 8.3 million U.S. adults discovered they were victims of some form of identity theft, causing them to spend between \$1,200 and \$2,000 and 55-130 hours to recover.¹ Researchers have estimated the total number of victims to be closer to 10 million with the total costs to individuals and businesses over \$50 billion a year. Under recently promulgated federal regulations, financial institutions and creditors, such as banks, finance companies, automobile dealers, mortgage brokers, utility companies, telecommunications companies, and including many doctors' offices, hospitals and other health care providers, are now required to implement a written program to detect, prevent and mitigate instances of identity theft. This article will briefly summarize two of the new federal regulations impacting Oklahoma businesses, the "Address Discrepancy Rule" and "Card Issuer Rule," and describe in detail the "Red Flags Rule."

BACKGROUND

On Nov. 9, 2007, the Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, the Office of Thrift Supervision, National Credit Union Administration and Federal Trade Commission (FTC) (collectively, the agencies) jointly issued an Identity Theft Red

Flags and Address Discrepancies Final Rule (the Final Rule)² and Interagency Guidelines (guidelines) — implementing Section 114 of the Fair and Accurate Credit Transactions Act of 2003 (the FACT Act)³ and Section 315 of the FACT Act. The FACT Act added new sections to the federal Fair Credit Reporting Act⁴ intended primarily to help consumers fight the growing crime of identity theft. Improved accuracy,

privacy, limits on information sharing and new consumer rights to disclosure were also included in the FACT Act.

Section 114 of the FACT Act authorized the agencies to: (i) issue guidelines for use by financial institutions and creditors regarding identity theft with respect to their account holders or customers; (ii) prescribe regulations requiring financial institutions and creditors to establish reasonable policies and procedures for implementing the guidelines to identify possible risks to account holders or customers or to the safety and soundness of the institution or customers; and (iii) prescribe regulations that would require credit and debit card issuers to assess the validity of notifications of changes of address under certain circumstances. The Final Rule implementing Section 114 of the FACT Act requires each financial institution or creditor to develop and implement a written Identity Theft Prevention Program (Program) to detect, prevent and mitigate identity theft in connection with certain types of accounts (the Red Flags Rule). In addition, the Final Rule also describes reasonable policies and procedures that debit or credit card issuers must employ to assess the validity of notifications of change of addresses in certain circumstances (the Card Issuer Rule).

Section 315 of the FACT Act provided that if a person has requested a consumer report from a nationwide consumer reporting agency (CRA), and the request includes an address for the consumer that substantially differs from the addresses in the file of the consumer, and if the CRA provides a consumer report in response to the request, the CRA must notify the requesting party of the existence of the discrepancy. The Final Rule implementing Section 315 of the FACT Act describes reasonable policies and procedures that a user of consumer reports, such as a creditor or employer, must utilize when a CRA sends the user a notice of address discrepancy (the Address Discrepancy Rule).

The Final Rule became effective Jan. 1, 2008, with mandatory compliance on Nov. 1, 2008. However, on Oct. 22, 2008, the FTC issued an enforcement policy statement that delays enforcement of the Red Flags Rule until May 1, 2009.⁵ However, note that this does not affect enforcement of the Address Discrepancy and Card Issuer Rules. Nor does it affect compliance for entities not under the jurisdiction of the FTC. The salient provisions of these rules are summarized below.

ADDRESS DISCREPANCIES

Under the Address Discrepancy Rule, a user of consumer reports must develop and implement reasonable policies and procedures — designed to enable the user to form a reasonable belief that a consumer report relates to the consumer about whom it has requested the consumer report when the user receives a notice of address discrepancy. A “notice of address discrepancy” means a notice sent to a user by a CRA pursuant to 15 U.S.C. § 1681c(h)(1) that informs the user of a substantial difference between the address for the consumer that the user provided when requesting the consumer report and the address in the CRA’s file for the consumer.

Examples of such reasonable policies and procedures include:

- 1) Comparing the information in the consumer report provided by the CRA with information it:
 - (a) Obtains and uses to verify the consumer’s identity in accordance with Customer Information Program (CIP) requirements⁶;
 - (b) Maintains in its own records, such as applications, change of address notifications, other customer account records, or retained CIP documentation; or
 - (c) Obtains from third-party sources; or
- 2) Verifying the information in the consumer report provided by the CRA with the consumer.

It is important to note that any employer who obtains a consumer report for employment purposes is considered a user of a consumer report. As a user of consumer reports, an employer is required to develop and implement these reasonable policies and procedures designed to enable it to form a reasonable belief that the consumer report relates to the applicant/employee about whom it has requested the report.

A user may also be required to develop and implement reasonable policies and procedures for *furnishing* an address for the consumer that the user has reasonably confirmed is accurate to the CRA from whom it received the address discrepancy notice. Among other reasonable

means, a user may reasonably confirm that an address is accurate by verifying the address with the consumer, reviewing its own records to verify the consumer's address, or verifying the address through third-party sources. Further, these policies and procedures must provide that the user will furnish the confirmed address to the CRA as part of the information that the user regularly furnishes for the reporting period in which it establishes a relationship with the consumer. However, this obligation to reasonably confirm and report the address only arises when the user:

- can form a reasonable belief that the consumer report relates to the consumer about whom the user requested the report;
- establishes a continuing relationship with the consumer; and
- regularly and in the ordinary course of business furnishes information to the CRA from which the address discrepancy notice relating to the consumer was obtained.

IDENTITY THEFT RED FLAGS

Introduction

Each financial institution⁷ or creditor⁸ that offers or maintains one or more "covered accounts" is required to develop and implement a written Identity Theft Prevention Program (program). This program must be designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or any existing covered account. "Identity theft" has the same meaning as in 16 C.F.R. § 603.2(a), which is a fraud committed or *attempted* using the identifying information of another person⁹ without authority. The program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities.

To determine whether it must develop a program, each financial institution or creditor must periodically determine whether it offers or maintains covered accounts. As part of this determination, the financial institution or creditor must conduct an initial risk assessment to determine whether it offers or maintains such accounts — taking into consideration the methods that it provides to open or access its accounts and its previous experiences with identity theft.

“A ‘red flag’ is a pattern, practice or specific activity that indicates the possible existence of identity theft.”



Definition of an 'Account' and a 'Covered Account'

An "account" means a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household, or *business* purposes. An account includes an extension of credit,¹⁰ such as the purchase of property or services involving a deferred payment and a deposit account.

A "covered account" is an account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions, such as the following types of accounts:

- credit card account
- mortgage loan
- automobile loan
- margin account
- cell phone account
- utility account
- checking account
- savings account

The term also includes any other account that the financial institution or creditor offers or maintains for which there is a *reasonably foreseeable risk* to customers (a person that has a covered account with a financial institution or creditor) or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation or litigation risks.

Elements of the Identity Theft Prevention Program

The program must include reasonable policies and procedures to:

- identify relevant red flags for the covered accounts that the financial institution or creditor offers or maintains, and incorporate those red flags into the program;
- detect red flags that have been incorporated into the program;
- respond appropriately to any red flags that are detected, in order to prevent and mitigate identity theft; and
- ensure that the program (including the red flags determined to be relevant) is updated periodically to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft.

A “red flag” is a pattern, practice or specific activity that indicates the *possible* existence of identity theft. Each financial institution or creditor that is required to implement a program must provide for the continued administration of the program, and must:

- obtain approval of the initial *written* program from either its board of directors¹¹ or an appropriate committee thereof;
- involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the program;
- train staff, as necessary, to effectively implement the program; and
- exercise appropriate and effective oversight of service provider¹² arrangements.

PROGRAM GUIDELINES

Introduction

Each financial institution or creditor that is required to implement a program must consider the guidelines described below and include in its program those guidelines that are appropriate. In addition to following the guidelines 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.

Identifying Relevant Red Flags

A financial institution or creditor should consider the following factors in identifying relevant red flags for covered accounts, as appropriate:

- the types of covered accounts it offers or maintains;
- the methods it provides to open its covered accounts;
- the methods it provides to access its covered accounts; and
- its previous experiences with identity theft.

Relevant red flags should be incorporated from sources such as: (i) incidents of identity theft that the financial institution or creditor has experienced; (ii) methods of identity theft that the financial institution or creditor has identified that reflect changes in identity theft risks; and (iii) applicable supervisory guidance. The program should also include, as appropriate, relevant red flags from the five categories noted below. The guidelines provide illustrative examples of red flags within each category which a financial institution or creditor may consider incorporating into its program, whether singly or in combination.

1. Alerts, Notifications or Other Warnings from CRAs or Service Providers

Alerts, notifications and other warnings received from CRAs or service providers, such as fraud detection services, should be included in the program, including:

- a fraud or active duty alert included with a consumer report;



- a notice of credit freeze provided by a CRA in response to a request for a consumer report;
- a notice of address discrepancy provided by a CRA; or
- a consumer report indicating a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as a recent and significant increase in the volume of inquiries, an unusual number of recently established credit relationships, a material change in the use of credit, especially with respect to recently established credit relationships, or an account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

2. Presentation of Suspicious Documents

Red flags associated with the presentation of suspicious documents should be addressed in the program, including:

- identification documents that appear to have been altered or forged;
- the photograph or physical description on identification documents that is not consistent with the appearance of the applicant or customer presenting the identification;
- other information on the identification documentation that is not consistent with information provided by the person opening a new covered account or customer presenting the identification;
- other information on the identification documentation that is not consistent with readily accessible information on file with the financial institution or creditor, such as a signature card or a recent check; or

- an application that appears to have been altered or forged, or that gives the appearance of having been destroyed and reassembled.

3. Presentation of Suspicious Personal Identifying Information

The presentation of suspicious personal identifying information, such as a suspicious address change, should be considered for inclusion in the program. Red flag examples include:

- personal identifying information provided that is inconsistent when compared against external information sources used by the financial institution or creditor. For example, an address that does not match any address in the consumer report or the Social Security Number (SSN) provided has not been issued or is listed on the Social Security Administration's Death Master File;
- personal identifying information provided by the customer that is not consistent with other identifying information provided by the person (for example, there is a lack of correlation between the SSN range and the date of birth);
- 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, when the address or phone number on an application is the same address or phone number provided on a fraudulent application;
- personal identifying information of a type commonly associated with fraudulent activity, as indicated by internal or third-party sources used by the financial institution or creditor – such as an address on an application that is fictitious, a mail drop or a prison, or a telephone number that is invalid or associated with a pager or answering service;
- the submission of a SSN that is the same as that submitted by other persons opening an account or other customers;
- the submission of an address or telephone number that is the same as or similar to the address or telephone number submitted by an unusually large number of other persons opening accounts or other customers;

- 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;
- the provision of personal identifying information that is not consistent with personal identifying information on file with the financial institution or creditor; or
- for financial institutions and creditors that use challenge questions, cases where the person opening the covered account or the customer is unable to provide authenticating information beyond that which would generally be available from a wallet or consumer report.

4. Unusual Use of or Suspicious Activity Related to Covered Account

The unusual use of, or other suspicious activity related to a covered account, should also be addressed in the program. Examples could include circumstances where:

- shortly following the notice of a change of address for a covered account, the financial institution or creditor receives a request for a new, additional, or replacement credit card or a cell phone, or for the addition of authorized users on the account;
- a new revolving credit account is used in a manner commonly associated with known patterns of fraud. For example, if 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 the customer fails to make the first payment or makes an initial payment, but no subsequent payments;
- a covered account is used in a manner not consistent with established patterns of activity on the account. For example, non-payment when there is no history of late or missed payments, a material increase in the use of available credit, a material change in purchasing or spending patterns, a material change in electronic fund transfer patterns in connection with a deposit account, or a material change in telephone call patterns in connection with a cellular phone account;
- 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);

- mail sent to the customer is returned repeatedly as undeliverable even though transactions continue to be conducted in connection with the customer's covered account;
- the financial institution or creditor is notified that the customer is not receiving paper account statements; or
- the financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.

5. Notice from Customers, Victims, Law Enforcement, etc.

A response to notices 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, should be included in the program. These include a notification by a customer, a victim of identity theft, a law enforcement authority or any other person that the financial institution or creditor has opened a fraudulent account for a person engaged in identity theft.

Red Flag Detection

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:

- 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 CIP rules; and
- authenticating customers, monitoring transactions, and verifying the validity of address change requests, in the case of existing covered accounts.

Preventing and Mitigating Identity Theft

The program should also provide for appropriate responses to red flags that the financial institution or creditor has detected that are commensurate with the degree of risk posed. In determining an appropriate response, the financial institution or creditor should consider

aggravating factors that may heighten the risk of identity theft. These include a data security incident that results in unauthorized access to a customer's account records held by the financial institution or creditor, a 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 (*i.e.* phishing) or to a fraudulent Web site. Appropriate responses may include:

- monitoring a covered account for evidence of identity theft;
- contacting the customer;
- changing any passwords, security codes, or other security devices that permit access to a covered account;
- reopening a covered account with a new account number;
- not opening a new covered account;
- closing an existing covered account;
- not attempting to collect on a covered account or not selling a covered account to a debt collector;
- notifying law enforcement; or
- determining that no response is warranted under the particular circumstances.

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:

- the experiences of the financial institution or creditor with identity theft;
- changes in methods of identity theft;
- changes in methods to detect, prevent and mitigate identity theft;
- changes in the types of accounts that the financial institution or creditor offers or maintains; and
- changes in the business arrangements of the financial institution or creditor, including mergers, acquisitions, alliances, joint ventures and service provider arrangements.

Administering the Program

Oversight of the program by the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management is required and should include:

- assigning specific responsibility for the program's implementation;
- reviewing annual reports prepared by staff regarding compliance by the financial institution or creditor with its duties to detect, prevent and mitigate identity theft; and
- approving material changes to the program as necessary to address changing identity theft risks.

Staff of the financial institution or creditor responsible for the development, implementa-

“...creditors that violate the Final Rule may be subject to civil monetary penalties of up to \$3,500 per violation for ‘knowing’ violations.”

tion 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 its identity theft duties under the Red Flags Rule. The report should address material matters related to the program and should evaluate issues such as: (i) the effectiveness of the 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; (ii) service provider arrangements; (iii) significant incidents involving identity theft and management's response; and (iv) recommendations for material changes to the program.

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 take appropriate steps to prevent or mitigate identity theft.

Other Applicable Legal Requirements

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

- for financial institutions and creditors that are subject to 31 U.S.C. § 5318(g), filing a Suspicious Activity Report (SAR) in accordance with applicable law and regulations;
- 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 on a consumer credit report;
- implementing any requirements for furnishers of information to CRAs under 15 U.S.C. § 1681s-2, for example, to correct or update inaccurate or incomplete information, and to not report information that the furnisher has reasonable cause to believe is inaccurate; and
- 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.

DUTIES OF CARD ISSUERS REGARDING CHANGES OF ADDRESS

Under the Card Issuer Rule, a debit or credit card issuer must establish and implement reasonable policies and procedures to assess the validity of a change of address if it receives notification of a change of address for a consumer's debit or credit card account and, within a short period of time afterwards (during at least the first 30 days after it receives

such notification), the card issuer receives a request for an additional or replacement card for the same account.

Under these circumstances, the card issuer may not issue an additional or replacement card until, in accordance with its reasonable policies and procedures and for the purpose of assessing the validity of the change of address, the card issuer:

- notifies the cardholder of the request at the cardholder's former address or by any other means of communication that the card issuer and the cardholder have previously agreed to use and provides the cardholder a reasonable means of promptly reporting incorrect address changes; or
- otherwise assesses the validity of the change of address in accordance with its identity theft program policies and procedures.

Any written or electronic notice that the card issuer provides must be clear and conspicuous¹³ and provided separately from its regular correspondence with the cardholder.

In the alternative, a card issuer may satisfy these requirements if it validates an address pursuant to these methods when it receives an address change notification, but before it receives a request for an additional or replacement card.

PENALTIES FOR NONCOMPLIANCE

Although there are no criminal penalties for failing to comply with the Final Rule, financial institutions or creditors that violate the Final Rule may be subject to civil monetary penalties of up to \$3,500 *per violation* for "knowing" violations. There is no formal guidance on what constitutes "per violation." It is arguable to characterize a failure to comply with the Final Rule, such as implementing a program as required by the Red Flags Rule, as a single knowing violation. However, from an enforcement-avoidance perspective, the better practice is to characterize that failure as one violation per account. From discussions with an FTC staff attorney, this is the way the FTC would probably look at the situation if a creditor were in the unfortunate position of being on the wrong side of an enforcement action. There is also the possibility of state enforcement and state civil actions for violation of the Final Rule.

CONCLUSION

The Final Rule incorporates many common sense and obvious business practices that financial institutions and creditors have been following (e.g., declining to open an account when the applicant's identification document does not match his or her appearance or application). In this sense, few financial institutions or creditors will have to change their basic procedures. However, financial institutions and creditors should have written policies and procedures in place that comply with the Address Discrepancy Rule and Card Issuer Rule, as well as a written program to detect, prevent and mitigate identity theft. As noted above, compliance with the Final Rule became mandatory on Nov. 1, 2008. However, enforcement of the Red Flags Rule by the FTC has been delayed until May 1, 2009.

1. Federal Trade Commission 2006 Identity Theft Survey Report, November 2007, available at <http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf>.

2. Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003; Final Rule. 72 Fed. Reg. 63718 (Nov. 9, 2007), available at <http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf>.

3. Pub. L. 108-159, 117 Stat. 1952.

4. 15 U.S.C. 1681 *et seq.*

5. FTC Press Release dated Oct. 22, 2008, available at: <http://www.ftc.gov/opa/2008/10/redflags.shtm>. The FTC Enforcement Policy is available at: <http://www.ftc.gov/os/2008/10/081022idthefredflagsrule.pdf>.

6. See 31 U.S.C. § 5318(1) and 31 C.F.R. § 103.121.

7. The term "financial institution" is defined in the same manner as in 15 U.S.C. § 1681a(t), which defines the term to mean a state or national bank, a state or federal savings and loan association, a mutual savings bank, a state or federal credit union, or any other person that, directly or indirectly, holds a transaction account (as defined in section 19(b) of the Federal Reserve Act) belonging to a consumer.

8. The term "creditor" has the same meaning as in 15 U.S.C. § 1681a(r)(5) and includes entities such as banks, finance companies, automobile dealers, mortgage lenders, mortgage brokers, utility com-

panies and telecommunications companies. Note that 15 U.S.C. § 1681a(r)(5) defines the term "creditor" by reference to section 702 of the Equal Credit Opportunity Act, which in turn defines "creditor" rather broadly to mean: any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit. 15 U.S.C. § 1691a(e).

9. A "person" is not limited to an individual; it could also be a partnership, corporation, trust, estate, cooperative, association, government or governmental subdivision or agency, or other entity. 15 U.S.C. § 1681a(f).

10. "Credit" has the same meaning as in 15 U.S.C. § 1681a(r)(5), which defines the term "credit" by reference to section 702 of the Equal Credit Opportunity Act, which construes "credit" to mean the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefor. 15 U.S.C. § 1691a(d).

11. "Board of directors" means in the case of a branch or agency of a foreign bank, the managing official in charge of the branch or agency, and in the case of any other creditor that does not have a board of directors, a designated employee at the level of senior management.

12. A "service provider" is a person that provides a service directly to the financial institution or creditor.

13. "Clear and conspicuous" means reasonably understandable and designed to call attention to the nature and significance of the information presented.

ABOUT THE AUTHOR



Eric L. Johnson is a shareholder with Phillips Murrah P.C. He has 15 years of experience providing commercial and consumer credit compliance advice on federal and state laws and regulations. He is a registered lobbyist, an adjunct professor of consumer law for Oklahoma City University School of Law and chairs the Legal Committee for the National Automotive Finance Association. He is a frequent speaker and author on consumer financial services issues.



GUNGOLL JACKSON
GUNGOLL JACKSON COLLINS BOX & DEVOLL, P.C.
ATTORNEYS & COUNSELORS AT LAW
Enid • Oklahoma City

Gungoll, Jackson, Collins, Box and Devoll, P.C. Attorneys at Law Welcomes Attorney John R. Morris

Attorney John R. Morris has over 25 years of practice and has successfully tried over 100 civil and criminal cases. He joined the law firm of Gungoll, Jackson, Collins, Box & Devoll, P.C. in August of 2008 and is the senior trial lawyer in its Oklahoma City office. A 1980 graduate of the University of Oklahoma College of Law, Mr. Morris has contributed numerous articles to professional publications and presented various trial-related subjects at continuing legal education seminars in Oklahoma.

Gungoll, Jackson, Collins, Box and Devoll, P.C., Attorneys and Counselors at Law
323 West Broadway, Enid OK • 580-234-0436 • 1-800-725-0436
Oklahoma City Office
100 N. Broadway, 3030 Chase Tower, Oklahoma City OK • 405-272-4710
www.GungollJackson.com