6 The Legal Environment of Credit

Overview

There is a critical need to be aware of the specific government legislation that pertains to business credit. Government legislation not only creates and protects the rights of creditors but also imposes limitations on business activities. Credit department policies and procedures should be in place to ensure that all actions taken by the department and its employees are within the boundaries of the law.

THINK ABOUT THIS

Q. How has human behavior influenced the evolution of laws in the business environment?

Q. How has technology influenced the business and legal environment?

DISCIPLINARY CORE IDEAS

After reading this chapter, the reader should understand:

- The four cornerstone federal antitrust acts and why they were written into law.
- The Fair Credit Reporting Act and its applications in consumer and commercial credit.
- The applicable practices a creditor must follow under the ECOA and Regulation B.
- The purpose of the Consumer Financial Protection Bureau.
- The rules that a creditor must follow under the Fair Debt Collection Practices Act when collecting from a debtor.
- What information a creditor must disclose to a consumer applying for credit under the Truth in Lending Act and Regulation Z.
- What constitutes an e-signature and its relevant provisions.
- The procedures and requirements a holder of unclaimed property must follow.
- Why SOX was enacted and its requirements for corporate responsibility and accountability.
- The Red Flags Rules.

Chapter Outline

1.	Antitrust Legislation	6-2
2.	The Fair Credit Reporting Act	6-6
3.	The Equal Credit Opportunity Act and Regulation B	6-8
4.	Dodd-Frank Wall Street Reform and Consumer Protection Act	6-13
5.	The Fair Debt Collection Practices Act	6-14
6.	The Truth in Lending Act and Regulation Z	6-15
7.	E-Sign Act	6-17
8.	Unclaimed Property Law (Escheatment)	6-19
9.	Sarbanes-Oxley Act of 2002	6-23
10.	Red Flags	6-25

Antitrust Regulation

Antitrust laws were initially enacted around the turn of the 20th century in response to the damaging effects that powerful monopolies, formed by corporate giants and others in the mid- to late-19th century, were having on small businesses. After the industrial revolution, monopoly power, along with many unfair trading practices such as price fixing and restraint of trade, was used to drive small businesses out of business. When monopolies were recognized as being out of control and damaging competition, federal antitrust laws started to appear in the United States to protect smaller businesses.

Four major federal acts have been passed over the course of the 20th century, each of which refined former laws by eliminating loopholes and establishing new provisions. These are the Sherman Act, the Clayton Act, the Robinson-Patman Act and the Federal Trade Commission Act. This chapter presents a summary of the four acts; the Acts are extremely complex and legal counsel should be sought when dealing with them. *The purpose of U.S. antitrust law is to encourage and protect competition.*

Comprehension Check
What is the purpose of **U.S. antitrust law?**

The latest edition of NACM's *Manual of Credit and Commercial Laws* is a source of additional information about these Acts.

The Sherman Act of 1890

The Sherman Act (15 USC §§1-7) was the first antitrust act passed in the United States. The Act was designed to prevent monopolies and unfair restraints of trade. *The Sherman Act prohibits contracts, combinations and conspiracies in restraint of trade in interstate commerce. It declares that every person who shall monopolize, or attempt to monopolize, or combine or conspire with any other person or persons, to monopolize any part of the trade or commerce among the several states, or with foreign nations, shall be deemed guilty of a felony, and, on conviction thereof, shall be punished by fine not exceeding $100,000,000 if a corporation, or, if any other person, $1,000,000, or by imprisonment not exceeding 10 years, or by both said punishments, in the discretion of the court.* In order for an offense to be considered a crime under the Sherman Act, a contract, combination or conspiracy between two or more persons or companies that has the effect of restraining or monopolizing trade or commerce within several states or with foreign nations must be made.

The purpose of the Sherman Act is to prohibit monopolies, contracts and combinations that would unduly interfere with the free exercise of their rights by those engaged, or who wish to engage, in trade and commerce; in short, its purpose is to preserve the right of freedom of trade. A seller of goods does not violate the Act by refusing to sell to others and may withhold goods from those who will not sell them at the prices suggested for their resale.

In determining if an action constitutes a conspiracy to commit an action that results in a restraint of trade, four elements must exist:

1. There must be knowledge of all the parities;
2. A common purpose;
3. An actual restraint of trade; and
4. Intent to restrain trade.

In short, the Sherman Act outlaws every contract, combination, or conspiracy in restraint of trade, and any monopolization, attempted monopolization, or conspiracy or combination to monopolize. Long ago, the Supreme Court decided that the Sherman Act does not prohibit *every* restraint of trade, only those that are *unreasonable*. For instance, in some sense, an agreement between two individuals to form a partnership restrains trade, but may not do so unreasonably and may be lawful under the antitrust laws. On the other hand, certain acts are considered so harmful to competition that they are almost always illegal. These include plain arrangements among competing individuals or businesses to fix prices, divide markets, or rig bids. These acts are *"per se"* violations of the Sherman Act; in other words, no defense or justification is allowed.

Comprehension Check
What is the **Sherman Act** designed to prevent?

The Business Environment in the Early 1900s

In the early 1900s, entrepreneurs wanted to expand by buying other companies, which created new lending opportunities for New York bankers. The most powerful and wealthy of these entrepreneurs were called robber barons. The term robber baron described businessmen who allegedly used unscrupulous tactics in their business operations and on the stock market to amass huge personal fortunes.

In 1901, John Pierpont Morgan created U.S. Steel, the first billion-dollar corporation. U.S. Steel was a giant integrated steel trust. Capitalized with $1.4 billion at a time when the capitalization of all American manufacturing was $9 billion, U.S. Steel elevated both Wall Street and U.S. industry to a new plateau. When it came time for J.P. Morgan to sell U.S. Steel, approximately 300 underwriters disposed of the securities.

Many of the robber barons' massive businesses controlled a large majority of all activity in their respective industries, often arrived at through predatory pricing schemes that are now illegal. Some of the most notable were J.P. Morgan (banking), John D. Rockefeller (oil), and Andrew Carnegie (steel).

The Clayton Act of 1914

The Clayton Act finds its roots in the 1912 presidential election when the three parties at the time, the Republicans, Democrats and Progressives, promoted the position that the Supreme Court had been too lenient on large corporations and that antitrust laws needed to be strengthened. **The Clayton Act** (15 USC §§12-27 and 29 USC §§52-53) followed the Sherman Act and *was created to correct defects in the Sherman Act. It also supplemented the Sherman Act by giving certain administrative agencies the power to stop violations of the law in their development and before a threatened conspiracy ripened into actuality*. Congress passed the Clayton Act to promote competition through protection of viable, small, locally owned businesses.

Under the Clayton Act, it is unlawful to enter into:

1. Leases or sales on condition that lessee or purchaser shall not use or deal in the commodities of a competitor of the lessor or seller;
2. Exclusive dealing arrangements; and
3. Tying arrangements (an agreement by a party to sell one product but only on the condition that the buyer also purchases a different (or tied) product).

In addition, the Clayton Act restricts the acquisition of stock by one corporation from another where the effect of such acquisition may be substantially to lessen competition or to tend to create a monopoly. The Clayton Act prohibits any person serving as a director or officer in any two corporations under certain conditions where their service would result in an elimination of competition that would violate any of the antitrust laws. The Act was amended in 1955 to add two new subdivisions: The first gives the United States a right of action for actual damages sustained by reason of any violation of any antitrust law; the second amendment imposes a four-year statute of limitations on actions by private persons or by the United States to recover damages under the Act.

The Clayton Act is a major civil statute intended to protect competition and to keep prices from skyrocketing due to mergers, acquisitions, or other business practices. By giving the government the authority to challenge large-scale moves made by corporations, the Clayton Act provides a barrier against monopolistic practices. Section 7 of the Clayton Act prohibits mergers and acquisitions where the effect is to substantially reduce competition or to create a monopoly.

An illustration of the use of the Clayton Act is the action taken by the Department of Justice to block the acquisition of General Electric Company's appliance business by AB Electrolux and Electrolux North America Inc., whose brands include Frigidaire. The Justice Department argued that the $3.3 billion acquisition would combine two of the leading manufacturers of ranges, cooktops and wall ovens sold in the United States, eliminating competition that has benefited American consumers through lower prices and more options. The Department argued that purchasers in the United States spent over $4 billion on these major cooking appliances in 2014. The Justice Department took the position that Electrolux's proposed acquisition of General Electric's appliance business would leave millions of Americans vulnerable to price increases for ranges, cooktops and wall ovens, which are products that serve an

important role in family life and represent large purchases for many households. The lawsuit also sought to prevent a duopoly in the sale of these major cooking appliances to builders and other commercial purchasers, who often pass on price increases to home buyers or renters. Ultimately, the acquisition was stopped and General Electric agreed to sell its appliance unit to Chinese manufacturer Haier Group.

The Federal Trade Commission Act of 1914

The Federal Trade Commission Act (15 USC §45) was the broadest of the important antitrust acts to be passed. *Its prohibitions include false advertising of foods, drugs, devices and cosmetics, and any other practice that is designed to deceive the public.* An example of an FTC Act claim, using Section 5, is a ''Made in USA'' claim in advertising and labeling.

Any practice that violates the Sherman Act, the Clayton Act or the Robinson-Patman Act—or even if it falls short of a violation but is related to the type of practice which they prohibit—may constitute an unfair method of competition in violation of the Federal Trade Commission Act. The ultimate aim of the Act is to protect the public from the actions likely to result from the destruction of competition or the restriction of competition to a substantial degree.

When the FTC was created in 1914 by this Act, its purpose was to prevent unfair methods of competition in commerce as part of the battle to bust the trusts. Over the course of time, Congress passed additional laws giving the agency greater authority to police anticompetitive practices. In 1938, Congress passed the Wheeler-Lea Amendment which included a broad prohibition against unfair and deceptive advertising practices. Since then, the Commission also has been directed to administer a wide variety of other consumer protection laws, including the Telemarketing Sales Rule, the Pay-Per-Call Rule and the Equal Credit Opportunity Act. In 1975, Congress gave the FTC the authority to adopt industry-wide trade regulation rules.

The Robinson-Patman Act of 1936

The Robinson-Patman Act (15 USC §13) was passed to supplement the Clayton Act. *The Robinson-Patman Act declares that it is unlawful for any person engaged in commerce or in the course of such commerce, either directly or indirectly, to discriminate in price between different purchasers of commodities of like grade and quality when either or any of the purchasers involved in such discrimination are engaged in interstate commerce, and where the commodities are sold for use, consumption or resale within the United States or any other place within its jurisdiction. This Act forbids price discrimination where the effect of such price discrimination is to substantially reduce competition or to create a monopoly in any line of commerce, or to injure, destroy or prevent competition with any person who either grants or knowingly receives the benefit of such discrimination or with customers of either of them.*

The Robinson-Patman Act is of particular importance to credit professionals. The term price discrimination includes the following types of business practices:

- **A different price charged to different purchasers.** A difference in price can only lawfully occur when the price difference results from differences in the cost of manufacture, sale or delivery resulting from the differing methods or quantities in which such goods are sold.
- **Differences in terms and conditions of sale.** For example, granting one purchaser free freight while charging freight costs to another is discriminatory.
- **Preferential credit terms.** Requiring one dealer to pay COD (cash upon delivery) while granting another dealer credit terms can support a price discrimination claim. Likewise, granting different credit terms to similar customers can be found to be discriminatory pricing. A creditor is entitled, however, to extend different terms to competing purchasers as long as the credit decision is made in a reasonable, nondiscriminatory manner so that the same standards of creditworthiness are applied to all customers who compete with each other.
- **Credit terms are an inseparable part of price according to a 1980 Supreme Court decision.** Anytime credit terms are fixed or adjusted, a price is being fixed. Allowing a customer to

pay in 30 days, giving that customer the use of that money for that period of time, is of monetary value. There is a difference between COD and credit terms.

Comprehension Check
What does the **Robinson-Patman Act** specifically forbid?

Antitrust Regulations and Credit

Price-fixing

Perhaps the most serious of antitrust violations in which credit grantors can find themselves engaged is **price-fixing.** In the 1980 case of *Catalano Inc. v. Target Sales,* the United States Supreme Court held that *it is virtually self-evident that extending interest-free credit for a period of time is equivalent to giving a discount equal to the value of the use of the purchase price for that period of time.* The Supreme Court said that the terms of credit are an inseparable part of the price paid for a product. Since price-fixing is automatically illegal under federal antitrust law; the court said that credit-fixing must also be illegal. Therefore, credit terms must be characterized as an inseparable part of the price.

Price Discrimination

For any person to be found liable for **price discrimination,** there is no need for there to be an agreement, combination, association, or conspiracy. In order for a violation to occur, the person accused of price discrimination must have engaged in at least two transactions, crossing state lines and both of these sales must be for use, consumption or resale within the United States.

While the Robinson-Patman Act specifically states that it is unlawful for any person to discriminate in price between different purchasers of commodities of like grade and quality or to knowingly grant or receive a benefit from such discrimination, the case law that has resulted from the statute has broadened the definition of price discrimination and the kinds of transactions that will be included in that definition. The term, price discrimination, now includes the following types of business practices:

A different price charged to different purchasers

The Robinson-Patman Act clearly states that a difference in price can only occur when the price difference results from differentials in the "cost of manufacture, sale, or delivery resulting from the differing methods or quantities in which such" goods are sold. Price changes are allowable when they result from "changing conditions affecting the market for or the marketability of the goods concerned" [15 USC §13(a)].

Differences in terms and conditions of sale

Granting one purchaser free freight while charging freight costs to another purchaser is discriminatory. Charging one price for goods "delivered" to a customer and charging the same price for goods "delivered f.o.b. terminal" has been found to be discriminatory.

Preferential credit terms

Requiring one dealer to pay COD while granting another dealer credit terms can support a price discrimination claim. Likewise, granting different credit terms to similar customers can be found to be discriminatory pricing. Any person is entitled to extend different terms to competing purchasers as long as the credit decision is made in a nondiscriminatory manner so that the same standards of creditworthiness are applied to all customers who compete with each other. For example, history of late payments and financial difficulties are sufficient business justification for denial of credit.

Credit executives are not immune from antitrust responsibilities; it is not only the sales department that can be found culpable for antitrust activity. Through the years of case law, the courts have come to hold one doctrine to be true, time and time again: credit terms equal price.

Permissive Granting of Preferential Credit Terms

Meeting competition is the likeliest defense to a claim of unlawful price discrimination. While there are various criteria that must be met in order for this defense to be properly used, here are some primary ones:

Good Faith. A credit grantor (seller) must prove that it had good reason to believe that it is meeting an equal credit term (or price). The standard is that of a prudent business person responding simply and fairly to what is reasonably believable.

Verifying Competitive Offers. It is common knowledge and readily understood that written verification of a competitive offer by the buyer is not going to be forthcoming. Credit professionals should not contact competitors for this information, but there should be well-documented information on the steps that led to the decision to meet a lower offer or better credit terms. It is recommended that a record containing the following information be created and maintained:

- The date of the competitor's offer.
- The name of the competitor making the offer.
- The name of the customer.
- The terms and conditions of the offer.
- The source of the information.
- A statement as to why the source (e.g., Company X has been a customer for five years and has always been truthful. Therefore, there is no reason not to believe the customer at this time.)

Legitimate Business Reason. A price discrimination claim can also be defeated if the seller can prove there was a cost justification for giving a different price (credit term). The details required to establish this defense will be:

- Differences in the cost of manufacturing, sale or delivery.
- That difference resulted from market conditions (e.g. deterioration of products, seasonal goods, discontinued items).
- Establishing credit for a financially healthy customer while requiring a financially troubled company to pay COD or CIA (cash-in-advance) is legitimate because it is based on the company's credit risk.

Comprehension Check
What types of business practices does the term **price discrimination** include?

Other Important Antitrust Legislation

Passed in 1974, **The Antitrust Procedures and Penalties Act** increased the penalties for offenses under the Sherman Act, changed consent decree procedures and revised the provisions for appellate review of antitrust cases. **The 1976 Antitrust Act** *grants the federal government new disclosure powers in antitrust litigation.* It also requires companies of a certain size to file pre-merger notices, and it permits a state attorney general to sue for damages on behalf of the state's residents. In addition to the above laws, almost all states have statutes prohibiting monopolies, contracts, conspiracies and combinations in restraint of trade.

Antitrust laws are complex and legal counsel should be consulted when dealing with them. Credit professionals should refer to the full text to ensure a thorough understanding of the Acts.

The Fair Credit Reporting Act

The Fair Credit Reporting Act (FCRA) is Title VI of the Consumer Credit Protection Act and became effective on April 25, 1971. *The purpose of the Act is to require consumer reporting agencies to adopt reasonable procedures that meet the needs of consumer credit, personnel (employment), insurance and other information that is fair and equitable to consumers.* The FCRA guarantees consumers the right to know what credit information credit bureaus and

consumer reporting agencies maintain and to receive a specific reason why they, as consumers, were denied credit. The Act was intended to apply only to consumer credit transactions and not to commercial credit transactions.

Amendments to the FCRA were created by the Consumer Credit Reporting Reform Act of 1996, which took effect on October 1, 1997. The amendments to the Fair Credit Reporting Act deal with personal or consumer credit that is defined as "credit for personal, family or household purposes." The extension of business credit, provided that it does not cross over into consumer credit, is not affected by the amendments.

Since the law does not focus on the nature of the proposed or actual credit recipient (individual, partnership or corporation) but rather focuses on the use of credit (personal, family or household purposes), it does not affect credit extended to individuals who may be sole proprietors of businesses or partners in a partnership operating a business. It is important for the credit grantor to be certain that the credit extension is for business purposes. A one or two sentence certification to that effect on a credit application or other written document ensures that the credit grantor is protected. A credit extension is not for personal, family or household purposes if a credit grantor receives a sales tax or other type of tax exemption from the credit recipient.

If a creditor is seeking a credit bureau report containing consumer credit information, then the individual about whom the information is sought should sign a written consent. The law makes it clear that the use of a consumer credit report may not be initiated or requested without the written authorization of the individual involved unless there is a permissible business use specifically defined by the statute. These permissible purposes include the use of the information for the extension and/or review of business credit, employment purposes and the underwriting of insurance involving the consumer.

The law deals with the duties involved in connection with information provided to credit reporting agencies for consumer credit reports and furnished by consumer reporting agencies. As long as the information provided by a credit reporting agency or in connection with an industry group credit exchange is based upon credit for commercial purposes and not for personal, family or household purposes, the statute's regulations do not apply. Because the law only deals with consumer credit that is limited to personal, family or household purposes, there has been no change in the long-standing practice concerning the absence of a requirement to provide information or justification for a business credit decision. This is a complicated area that requires the advice of counsel should a particular issue arise.

Under Section 604(3)(F) of the Fair Credit Reporting Act, the requesting creditor may only request a consumer report if there is a legitimate business need for the information, meaning that the need is:

1. In connection with a business transaction that is initiated by the consumer; or
2. To review an account to determine whether the consumer continues to meet the terms of the account.

Generally, the consumer reporting agency will require the requesting creditor to certify the permissible purpose for which the report is being obtained and must certify that the report will not be used for any other purpose. Should this certification be inaccurate or incomplete, the credit grantor requesting the report can be held liable.

The term, consumer report, is defined in the law to mean any written, oral or other communication of any information by a consumer reporting agency detailing a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living that is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for:

- Credit or insurance to be used primarily for personal, family or household purposes.
- Employment purposes or any other purpose authorized under Section 604.

In general, a consumer reporting agency may not furnish a report unless the consumer has initiated the transaction or has authorized the agency to provide the report or the transaction consists of a firm offer of credit or insurance and other applicable provisions are met:

Comprehension Check

What is the purpose of the **Fair Credit Reporting Act?**

- Extension of credit, or review or collection of an account of the consumer; or
- Intends to use the information for employment purposes.

The Equal Credit Opportunity Act and Regulation B

Purpose

The purpose of **The Equal Credit Opportunity Act and Regulation B (ECOA)** *is to promote the availability of credit to all creditworthy applicants without regard to race, color, religion, national origin, sex, marital status or age (provided the applicant has the capacity to contract).* It promotes the availability of credit without regard to the fact that all or part of the applicant's income derives from a public assistance program or to the fact that the applicant has, in good faith, exercised any right under the Consumer Credit Protection Act. The regulation also requires creditors to notify applicants of action taken on their applications and to retain records of credit applications.

The ECOA and Regulation B apply to all credit, commercial as well as personal, without regard to the nature or type of the credit or the creditor. It applies to credit extended to any individual, partnership or corporation for any purpose. It also applies to consumer leases. Each credit application, and all other means of obtaining information from a potential buyer, should also be evaluated to ensure compliance with ECOA requirements.

The wide breadth of the ECOA causes it to affect many businesses that routinely evaluate the creditworthiness of their customers. For this reason, it is important for all businesses involved in selling on credit to have procedures in place and employees trained in those procedures in order to ensure effective compliance with the law. Congress wrote the ECOA in broad language, and it is interpreted by Federal Regulation B in even more expansive terms.

All businesses that deal with any type of credit transaction need to be aware of the Act's provisions and be cognizant of simple steps they can take to avoid liability under the Act. Companies reviewing credit applications of their business customers are not immune from having charges made against them for ECOA violations. Many of these cases involve less visible ECOA provisions, such as its notification requirements. In a recent case brought in an Indiana federal court, the court found a bank liable under the Act for failure to provide a business applicant notice of an adverse action within 30 days.

Comprehension Check
What is the purpose of the **Equal Credit Opportunity Act?**

The Basic Rules of ECOA and Regulation B

Businesses may not refuse to grant business credit or discourage a business credit applicant from asking for credit based on sex, marital status, religion, etc. The basic rules of ECOA and Regulation B state that a business credit grantor cannot:

- Discriminate against an applicant regarding any aspect of a credit transaction.
- Make any oral or written statement, in advertising or otherwise, to applicants or prospective applicants, that would discourage a reasonable person from making or pursuing an application.
- Inquire whether income stated in an application is derived from alimony, child support, or separate maintenance payments unless the creditor discloses to the applicant that such income need not be revealed if the applicant does not want the creditor to consider it in determining the applicant's creditworthiness.
- Inquire about the sex of an applicant.
- Inquire about birth control practices, intentions concerning the bearing or rearing of children, or capability to bear children.
- Inquire about the race, color, religion or national origin of an applicant.
- Request any information about a spouse of an applicant unless the spouse will be permitted to use the account; the spouse will be contractually liable on the account; the applicant

is relying on the spouse's income as a basis for repayment of the credit requested; the applicant resides in a community property state, or property on which the applicant is relying as a basis for repayment of the credit requested is located in such a state; or the applicant is relying on alimony, child support, or separate maintenance payments from a spouse as a basis for repayment of the credit requested.

- Inquire about the applicant's marital status unless the applicant resides in a community property state, or is relying on property located in such a state as a basis for repayment of the credit requested.

Personal Guarantees

The last two factors listed also come into play on personal guarantees. The ECOA does not permit a credit grantor to require a spouse to sign a personal guarantee if that spouse is not directly involved with the business credit applicant. Care must be taken to make sure that there are policies established for dealing with this, so that there is not an accidental noncompliance.

The law does permit a spouse to sign a personal guarantee, if certain detailed procedures are followed to first verify that the applicant does not have the financial statement or credit wherewithal to support a guarantee. Once the fact is independently established that the applicant does not meet certain creditworthiness criteria, the business credit grantor would have to deny the request or ask for additional financial information to support the request. Should the applicant volunteer the additional guarantee of a spouse, even though that spouse is not directly involved in the business, it is permissible for the spouse to also sign the guarantee. The key is that the business credit grantor may not require a spouse to sign the guarantee; it must be voluntary. This is a very complicated procedure, and competent legal counsel should be consulted in order to establish the appropriate policies and procedures for each company.

Credit applications are not required, but if used, must conform to the requirements of Regulation B.

Notification of ECOA Compliance, Action Taken and Statement of Specific Reasons

For the purposes of notification to consumers, the Federal Reserve Board created a distinction for trade credit to differentiate it from other types of business credit. The Board defines **trade credit** *as limited to a financing arrangement that involves a buyer and a seller such as a supplier who finances the sale of equipment, supplies or inventory; it does not apply to an extension of credit by a bank or other financial institution for the financing of such items.* The Board defines **factoring** *as a purchase of accounts receivable, and therefore factoring is not subject to the Act or the Regulations.* If there is a credit extension incident to the factoring arrangement, then the notification rules and the relevant provisions of the ECOA apply.

The Board created this distinction between trade and business credit in the area of noticing to curb discriminatory practices against women and small businesses seeking **working capital** (*the capital of a business that is used in its day-to-day trading operations, calculated as the current assets minus the current liabilities*) or **venture capital** (*capital invested in a project in which there is a substantial element of risk, typically a new or expanding business*). All business creditors must notify credit applicants that they comply with the Equal Credit Opportunity Act. The easiest way to comply with this requirement is to add the following language to a credit application:

> Notice: The Federal Equal Opportunity Act prohibits creditors from discriminating against credit applicants on the basis of race, color, religion, national origin, sex, marital status, age (provided the applicant has the capacity to enter into a binding contract); because all or part of the applicant's income derives from any public assistance program; or because the applicant has, in good faith, exercised any right under the Consumer Credit Protection Act. The federal agency that administers compliance with the law concerning this credit is the Federal Trade Commission, Division of Credit Practices, 6th and Pennsylvania Avenue, NW, Washington, DC 20580.

Noticing Requirements Based on Gross Revenues of the Applicant

The Board establishes two types of business applicants.

1. Those with gross revenues of $1 million or less in their preceding fiscal year.

   A business credit (non-trade) grantor must notify applicant either orally or in writing within 30 days of receiving a completed application concerning the approval of, counter-offer to, or adverse action taken.

   If adverse action taken, within 30 days creditor must provide either statement of specific reasons for the action taken or disclosure of the applicant's right to a statement of the reasons for an adverse action. Notice of disclosure may be given at the time adverse action is taken or at the time the application is submitted provided that the disclosure is in a form the applicant may retain and contains the required ECOA notices.

Sample language of statement of specific reasons for action taken:

Thank you for applying to us for credit. We have given your request careful consideration and regret that we are unable to extend credit to you at this time for the following reasons:

Insert the appropriate reason, such as: value or type of collateral not sufficient, lack of established earnings record, slow or past due in trade or loan payments, etc.

Sample language of disclosure of applicant's right to request specific reasons for credit denial at time of application:

If your application for business credit is denied, you have the right to a written statement of the specific reasons for the denial. To obtain this statement, please contact [name, address and telephone number of the person or office from which the statement of reasons can be obtained] within 30 days from the date of this notification. We will send you a written statement of reasons for the denial within 30 days of receiving your request for the statement.

Insert the appropriate reason, such as: value or type of collateral not sufficient, lack of established earnings record, slow or past due in trade or loan payments, etc.

   For applications made solely by phone, a creditor may give an oral statement of the action taken and of the applicant's right to a statement of reasons for adverse action.

2. Those with gross revenues of more than $1 million in their preceding fiscal year. Small volume creditors are also given special noticing consideration.

   With respect to applications for trade credit, or for business credit, creditor must notify applicant either orally or in writing within a reasonable time of action taken. If applicant makes a written request for the reasons of the adverse action within 60 days, the creditor must give applicant a written statement of the specific reasons for the action and the ECOA notice.

Adverse Action

Four kinds of actions qualify as adverse:

1. A **refusal to grant credit** in substantially the amount or on substantially the terms requested in an application unless the creditor makes a counteroffer (to grant credit in a different amount or on other terms), and the applicant uses or expressly accepts the credit offered.
2. A **refusal to increase the amount of credit** available to an applicant who has made an application for an increase.
3. A **reduction of credit** availability on an existing account.
4. A **termination of an account** or an unfavorable change in the terms of an account that does not affect all or substantially all of a class of the creditor's accounts.

The following are *not* considered adverse actions:

1. A change in the terms of an account expressly agreed to by an applicant.
2. Any action or forbearance relating to an account taken in connection with inactivity, default, or delinquency as to that account.
3. A refusal or failure to authorize an account transaction at point of sale or loan except when the refusal is a termination or an unfavorable change in the terms of an account that does not affect all or substantially all of a class of the creditor's accounts or when the refusal is a denial of an application for an increase in the amount of credit available under the account.
4. A refusal to extend credit because applicable law prohibits the creditor from extending the credit requested.
5. A refusal to extend credit because the creditor does not offer the type of credit or credit plan requested.

Comprehension Check

The **ECOA** defines the term adverse action. List the four types of action that qualify as adverse under the ECOA.

Keeping Records

Business credit grantors must retain all information used in making a credit decision on an applicant for 12 months after the date on which the business credit grantor notifies the applicant of action taken on an application. However, for business applicants with gross revenues in excess of $1 million in its preceding fiscal year, creditors shall retain records for at least 60 days after notifying a business applicant. If, within that time period, the applicant requests in writing the reasons for adverse action or that the records be retained, the creditor must retain those records for 12 months.

Penalties

A creditor who violates a provision of the ECOA is liable for all actual damages sustained by the applicant either as an individual or as a member of a class. In addition to actual damages, punitive damages are also available. For creditors other than a government or governmental subdivisions or agency, punitive damages are capped at $10,000 for an individual creditor and $500,000 for a class action (or 1% of the net worth of the creditor).

Courts consider several factors when determining whether to award punitive damages and when determining the proper amount of punitive damages for violations of the ECOA. These factors include "the amount of any actual damages awarded, the frequency and persistence of failures of compliance by the creditor, the resources of the creditor, the number of persons adversely affected and the extent to which the creditor's failure of compliance was intentional." Additionally, it is important to note that attorneys' fees and costs are also available to plaintiffs in ECOA actions. In a recent Southern District of Indiana case, a plaintiff was awarded $10,000 in punitive damages and more than $55,000 in attorneys' fees and costs against a defendant creditor who failed to properly comply with the

Act's notice provisions. Therefore, it is important for companies to realize that once fees and costs are included, damages under the ECOA can be quite substantial.

Discrimination Measured by Effects Test

It is important to recognize that discrimination under the ECOA is measured by an "effects test" and is not simply based upon ill or malicious intent. Even if a creditor does not intentionally mean to discriminate, it can be held liable under the Act if the effects of its action result in discrimination toward one of the protected groups. To bring a suit under the ECOA, the plaintiff must:

1. Establish that it is a member of a protected class.
2. Demonstrate that it applied for and was denied credit.
3 Be denied credit.
4. Show that the creditor continued to approve credit applications for applicants with qualifications similar to those of the plaintiff.

Electronic Communication

Any disclosure required by Regulation B to be in writing may be provided by a creditor electronically in a clear and conspicuous manner and in a form the applicant may retain. A creditor must obtain an applicant's affirmative consent to obtain disclosures by electronic communications in accordance with the requirements of the E-Sign Act.

A creditor that uses electronic communication to provide disclosures shall:

- Send the disclosure to the applicant's electronic address; or
- Make the disclosure available at another location such as an Internet web site; and
- Alert the applicant of the availability of the disclosure by sending a notice to the applicant's electronic address (or to a postal address, at the creditor's option). The notice shall identify the account involved and the address of the Internet web site or other location where the disclosure is available; and
- Make the disclosure available for at least 90 days from the date the disclosure first becomes available or from the date of the notice alerting the applicant of the disclosure, whichever comes later.
- When a disclosure provided by electronic communication is returned to a creditor undelivered, the creditor shall take reasonable steps to attempt redelivery using information in its files.

Compliance

Compliance under the ECOA is not difficult, but it does require a review of current procedures to make sure effective procedures are in place. Establishing these now will protect a company in the event of a disgruntled customer down the road. There are five practices companies should adopt to make sure it limits liability under the Act.

1. Ensure that credit applications are worded neutrally, not asking for any prohibited information.
2. The criteria used to determine the creditworthiness of a potential customer must be easily measured and documented. Financial statements and financial references such as the customer's bank or other trade creditors from the buyer should be requested to assist in making a credit decision. Credit reports concerning the potential customer are another reliable source.
3. Establish and maintain a systematic method of complying with the Act's notification requirements. If a company determines that a customer is not creditworthy enough to

buy on credit, notify the potential buyer within the 30 days required under the Act. If the guarantee of an individual is requested, denials of the guarantor should be made timely. Incorporating a statement recording the date when the credit application was received and when notification was given is recommended.

4. Companies should develop a record retention policy that is in compliance with the Act.
5. Companies should educate employees about discrimination and require compliance with its notification and record retention policy.

Dodd-Frank Wall Street Reform and Consumer Protection Act

The Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank Act) *established the* **Consumer Financial Protection Bureau (CFPB).** While the CFPB's primary mission is related to consumer lending, its oversight applies to commercial lenders and trade creditors in limited instances. For example, the Dodd-Frank Act transferred rulemaking authority under both the ECOA and the Home Mortgage Disclosure Act to the CFPB. This authority gives the CFPB responsibility for preparing fair lending reports to Congress and forcing compliance with law that requires lenders to report accurate data to credit reporting agencies.

There are many instances when a commercial trade credit grantor obtains and uses a consumer credit report in making its decision to extend credit. These instances may include extending credit to a sole proprietor, extending credit to a "mom and pop" business which is an artificial entity (such as a corporation or limited liability company) or accepting a personal guarantee in order to extend credit to a business.

Keep in mind that the ECOA notifications and disclosures to a credit applicant are only applicable when the trade credit grantor makes an adverse credit decision. If credit is granted, these notifications and disclosures are not required. With respect to these notifications and disclosures, the Dodd-Frank Act caused changes to the Fair Credit Reporting Act, which also was originally created to protect consumers. These Dodd-Frank Act changes to the FCRA impact the ECOA.

The ECOA requires disclosure of the principal reasons for denying or taking other adverse action on an application for an extension of credit. The FCRA requires a creditor to disclose when it has based its decision in whole or in part on information from a source other than the applicant or its own files. Disclosing that a credit report was obtained and used in the denial of the application, as the FCRA requires, does not satisfy the ECOA requirement to disclose specific reasons. For example, if the applicant's credit history reveals delinquent credit obligations and the application is denied for that reason, to satisfy the ECOA, the creditor must disclose that the application was denied because of the applicant's delinquent credit obligations. The FCRA also requires a creditor to disclose, as applicable, a credit score it used in taking adverse action along with related information, including the key factors that adversely affected the consumer's credit score. Disclosing the key factors that adversely affected the consumer's credit score does not satisfy the ECOA requirement to disclose specific reasons for denying or taking other adverse action on an application or extension of credit. To satisfy the FCRA requirement, the creditor must also disclose that a credit report was obtained and used in the denial of the application.

Comprehension Check

What is the purpose of the **Dodd-Frank Wall Street Reform Act?**

If a consumer credit report was used by the trade credit grantor in making its credit decision, the following language should be included in the notification to the applicant:

Sample language of notification to applicant when using a consumer credit report

Our credit decision was based in whole or in part on information obtained in a report from the consumer reporting agency listed below. You have a right under the Fair Credit Reporting Act to know the information contained in your credit file at the consumer reporting agency. The reporting agency played no part in our decision and is unable to supply specific reasons why we have denied credit to you. You also have a right to a free copy of your report from the reporting agency if you request it no later than 60 days after you receive this notice. In addition, if you find that any information contained in the report you receive is inaccurate or incomplete, you have the right to dispute the matter with the reporting agency.

Name: _____

Address: _____

[Toll-free] Telephone number: _____

If the trade credit grantor uses a credit score in making the credit decision, the following additional language must be added to its notification:

Sample language of notification to applicant when using a credit score

We also obtained your credit score from this consumer reporting agency and used it in making our credit decision. Your credit score is a number that reflects the information in your credit report. Your credit score can change, depending on how the information in your credit report changes.

Your credit score: _____

Date: _____

Scores range from a low of _____ to a high of _____

Key factors that adversely affected your credit score:

_____

_____

_____

_____

[Number of recent inquiries on credit report]

The Fair Debt Collection Practices Act

The Fair Debt Collection Practices Act, (15 USC §§1692-1692) was passed in 1977 and became effective on March 20, 1978. *Commonly known as FDCPA, the Act was created to make fair laws for the benefit of debtors when a creditor attempts to recover debts.* Ordinarily, the Act only applies to "consumer" debts or those incurred primarily for personal, family or household purposes, even if the debts have been reduced to judgment.

The FDCPA focuses on the collection activities of third-party collectors such as collection agencies and attorneys. Ordinarily, creditors are exempt from the FDCPA if they are collecting their own debts in their own name. A creditor loses this exemption if it uses any name other than its own so as to make it appear that a third party is attempting

to collect its debts. Such conduct both violates the Act and renders the creditor liable to the same extent as a third-party debt collector.

Multiple cases have held that a creditor that purchases a debt after it is already in default will be treated as a debt collector under the Act and cannot maintain its creditor exemption. Therefore, companies that purchase portfolios of bad debts must ensure that their employees comply with the FDCPA.

The Federal Trade Commission has taken the position that the FDCPA may set standards for fair trade practices by creditors. The Commission has stated that under Section 5 of the FTC Act it could pursue creditors and collectors of commercial debts for the type of conduct that is prohibited by the FDCPA, even though such businesses are exempt from the FDCPA itself.

In addition to the FDCPA, many state laws restrict the actions of those who collect consumer debts. While there are many variations in the state statutes, both California and Pennsylvania have enacted statutes that apply the bulk of the FDCPA to creditors who are collecting their own debts in their own names. Texas, North Carolina and Florida have fair debt laws that impose substantial restrictions on creditors. Therefore, it is clear that a creditor that deals in retail debts would be wise to implement collection procedures that are consistent with the FDCPA.

Common FDCPA Prohibitions

The following is a partial list of the practices prohibited by the FDCPA:

- Misrepresenting the character or amount of a debt.
- Threatening to take action prohibited by law.
- Threatening to take action that is not intended to be taken.
- Using profane, obscene or abusive language.
- Making repeated calls for the purpose of harassment.
- Reporting a disputed debt to a credit bureau without disclosing that it is disputed.
- Reporting a "stale" debt to a credit bureau.
- Suing or threatening to file suit on a time-barred debt.
- Continuing to collect without first complying with a verification request.
- Communicating improperly with a third party.
- Communicating with a consumer who is known to be represented by an attorney.
- Communicating with a consumer at improper hours or at a time or place known to be inconvenient.
- Filing suit in an improper venue.
- Using any sort of false representations or deceptive means to collect a debt.

Businesses that violate the FDCPA can be sued for any actual damages resulting from the violation, together with statutory damages in the amount of $1,000 per suit and the attorney's fees incurred in prosecuting the suit. The Act also allows for class actions; in such an action suit, the defendant can be held liable for up to $500,000 or 1 percent of its net worth, whichever is less, plus the named plaintiff's individual claim and reasonable attorney's fees and costs incurred in pursuing the class action.

Comprehension Check

How does the **Fair Debt Collection Practices Act** affect the collection of a debt by a debt collector?

The Truth in Lending Act and Regulation Z

Congress passed **The Truth in Lending Act (TILA) Act** in 1968 with the intention of protecting and educating consumers in the field of purchasing credit. At the time, it was thought that the information given to consumers when purchasing credit was not thorough enough for them to establish whether or not they were receiving a good

deal. President Johnson wanted consumers to be able to examine the use of credit in much the same way as they might purchase any other product. This Act and its companion Regulation Z, which comprises the Act's rules and regulations, attempt to give consumers the opportunity and right to shop for credit.

In an effort to protect and educate consumers, *sellers of credit are mandated by law to disclose certain information when offering credit.* Such information allows consumers to know exactly what interest rates, finance charges and fees will apply before accepting such credit. This information provides consumers with the opportunity to shop around and find which rates, terms and conditions are the best for them. While this Act only applies to consumer credit, it is important to remember that many exemptions apply to the Truth in Lending Act and Regulation Z. For example, if a credit purchase is not used primarily for personal consumer use such as business or agricultural, then it may be deemed exempt under this title.

TILA and Regulation Z exempt credit transactions involving extensions of credit primarily for: business; commercial or agricultural purposes; or to government or governmental agencies or instrumentalities; or to organizations.

It also exempts:

- Transactions in securities or commodities accounts by broker-dealers registered with the Securities and Exchange Commission;
- Credit transactions, other than those in which a security interest is or will be acquired in real property or in personal property used or expected to be used as the principal dwelling of the consumer, in which the total amount financed exceeds $25,000; and
- Transactions under public utility tariffs, if the Board of Governors determines that a state regulatory body regulates the charges for the public utility services involved, the charges for delayed payment and any discount allowed for early payment.

Lastly, loans made, insured or guaranteed pursuant to a program authorized by Title IV of the Higher Education Act of 1965 are exempt under TILA and Regulation Z.

To protect consumers, the Act states that certain information must be disclosed to the applicant on the credit application: any finance charges that may or will be incurred (Regulation Z is very specific in explaining what charges may be considered finance charges and what charges are not) and the annual percentage rate (APR)—probably the most important disclosure mentioned in the Act. A consumer must know how much the APR is, whether it is paid yearly, quarterly or monthly, and so on. If an attempt is made by the issuer of credit to mask any information pertaining to charges to be incurred in the APR, they stand in clear violation of this Act. Other information that must be disclosed on the credit application is whether the consumer is applying for open-end or closed-end credit and what the differences between the two are.

Many rules must be followed under the title of the Truth in Lending Act and Regulation Z. Rules include the disclosure of particular information on applications for open-end consumer credit plans before a credit card is issued and periodic statements that must be sent to the consumer if an amount is owed at the end of a billing cycle. For closed-end credit disclosures, the disclosure must also be segregated from all other copy pertaining to the credit. If any part thereof is violated, a good chance exists that the **laws of usury,** *which pertain to the ceilings of interest rates,* have been violated as well. Different kinds of credit have different ceiling caps on allowable interest, which is a simple concept that becomes rather complicated very quickly. Although this doesn't directly deal with the Truth in Lending Act and Regulation Z, APR rates do make the two correlate on occasion. Therefore, it is pertinent that legal counsel be consulted when creating any documents that fall under the rules of TILA.

Comprehension Check
What is the purpose of the **Truth in Lending Act?**

The Fair Credit Billing Act

In 1975, the Truth in Lending Act was amended to create **The Fair Credit Billing Act.** The intention of this law is to take the hassle out of billing errors for consumers. *Creditors are required to correct errors promptly while at the same time preventing the errors from showing up on consumer credit reports.* Since this law was designed for consumer credit, discussion in this chapter is limited. For more information about the Fair Credit Billing Act,

please refer to the Federal Reserve Board website and its Consumer Handbook to Credit Protection Laws at www.consumerfinance.gov/creditcards.

E-Sign Act

Electronic signatures and records as well as agreements entered into electronically, such as via email and facsimile, are generally valid and enforceable as long as the sender intended to affix their signature to the document. There are both federal and state statutes in place that provide for the validity of electronic signatures and the enforcement of contracts entered into by electronic communications.

In 2000, Congress passed **The Electronic Signatures in Global and National Commerce Act,** known colloquially as the **"E-Sign Act."** The goal of Congress in enacting the E-Sign Act was to facilitate the continued success of electronic commerce, by making electronic transactions and signatures have the same legal standing as conventional paper ones.

The E-Sign Act set the enforcement of electronic communications in motion and provided a template for laws governing electronic signatures and communications subsequently put in place throughout the country. In Section 7001(a), the E-Sign Act provides:

1. A signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form; and
2. A contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation.

Comprehension Check
List two provisions of the **E-Sign Act.**

Electronic Signature Defined

In Section 7006(5), the **E-Sign Act** defines **electronic signature** *as an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.* The various statutes adopted by states around the country include similar definitions.

A basic principle of contract law known as the statute of frauds requires that certain types of contracts be in written form (as opposed to oral), including contracts for the sale of goods involving a minimum price. Various forms of communication, including letters, fax, telex and telegraph are regularly recognized by courts as fulfilling requirements in the Uniform Commercial Code (UCC) or other statutes that a contract be in writing. More recently, courts have added emails to that list and found that electronic signatures on emails and other documents are valid and enforceable as well, regardless of whether the signature is typed or written. Invoices, receipts, purchase orders, requisitions and agreements to purchase that are emailed, scanned, faxed or otherwise electronically transmitted can fulfill the requirement that a certain type of contract be in writing. Typically, courts have not required a written signature, finding that a typed signature is sufficient if the signatory acted with intent to sign.

The Validity of Electronic Communications

A string of emails or a confirmatory email setting forth the necessary contract terms may also constitute a valid and enforceable agreement entered into electronically. For example, the United States District Court for the Southern District of New York found in a case that emails between parties satisfied the signature and confirmation requirements of the statute of frauds because the company's president's typed signature appears at the signatory line of the attached letter and the letter is typed on company letterhead, the writing is sufficient against the sender. The court explained that the statute of frauds aims to guard against fraud and perjury by requiring some proof of contract, and the UCC's sale of goods provision is designed to require some objective guarantee, other than word of mouth, that there really has been some deal. An email suffices as much as a letter, a telegram or a fax to provide such objective indication of an existing agreement.

The validity of electronic communications is also relevant under a principle of contract law known as the merchant's exception, which permits enforceable contracts to emerge from the common commercial practice of entering into oral agreements for the sale of goods that are only later confirmed in writing. Finding that emails are commonly used by merchants and the public alike, the Southern District of New York found that emails can constitute the after-the-fact written confirmation under the merchant exception, and the email need only be sufficient against the sender. In most cases and depending on the applicable UCC or state contract law requirements, the email should include the subject of the contract, the specific terms of the agreement, and the price to be paid for the merchandise or products. In construing emails and electronic communications, courts have emphasized that, under the relevant state and federal statutes, the sender of the electronic communication must have intended to affix their signature.

Although emails between parties can constitute sufficient evidence of an agreement, the court found that an undated and unsigned letter sent attached to an email constituted an unbinding draft, rather than final letter, for a number a reasons. First, later letters were circulated on the issue indicating that the undated letter attached to the email was not the final word on the topic; second, the letter was written on letterhead for one entity over the name of a vice president for another entity, with no explanation of the named person's role in either entity; and third, the letter did not include a written signature but instead included a typed name, title and corporate affiliation in a format that would normally appear under a signature, not in place of one. With all of these reasons, the court found that there was "little or no evidence" that the alleged signatory to the letter intended to be bound.

Electronic Signatures in Commercial Transactions

Recognizing the growing use of electronic signatures in commercial transactions, a variety of applications and computer software programs now provide users with an easy platform to digitally insert signatures and electronically return signed documents, such as by email or facsimile. The best options of these types of platforms are those that warrant that they are fully compliant with the E-Sign Act and other similar statutes, such as DocuSign®. In addition, DocuSign® and a similar product, Adobe® EchoSign®, have created mobile applications for use on mobile applications to allow users to electronically sign and return documents at any moment, without any printing or scanning necessary.

Electronic Signatures and Credit

For the credit professional, an e-signature may eliminate a customer's need to download an application and mail the completed application with a handwritten signature. Some of the relevant provisions of the E-Sign Act are:

- Parties to the contract decide on the form of digital signature technology to validate the contract.
- Businesses may use e-signatures on checks.
- Businesses must require parties to the contract to make at least two clicks of a computer to complete a deal.
- The consumer decides whether to use an e-signature or handwritten signature.
- Cancellation and foreclosure notices must be sent on paper.
- E-signatures on adoptions, wills, and product safety recalls are not allowed.
- Records of e-contracts may be stored electronically.

In sum, electronic signatures are valid and enforceable so long as the signor intended to sign, and the party seeking to enforce the electronically signed agreement is able to reasonably demonstrate the signor's intent.

Comprehension Check

What are some advantages of **e-signatures?**

Unclaimed Property Law (Escheatment)

Post-September 11 and the States' Efforts to Find Untapped Revenue

States are incurring enormous financial costs for homeland security as a result of terrorist acts and are therefore looking for untapped revenue sources. The post-September 11 costs to state governments are estimated in the billions. For example, just New York property claims alone associated with the September 11 attacks reached into the billions. Local governments and cities report that municipal revenues have been affected by the September 11 attacks, and many are finding it difficult to meet budgets, in part, because of a decrease in tax collection and an increase in expenses to cover security. In this setting, states are looking for sources of revenue, and abandoned property, as the press reports, may be that untapped source for states. Escheatment revenue is an appealing revenue source from the states' view, as it does not require raising taxes. States are aggressive in their escheat efforts; several private firms are working on behalf of states on a contingency fee basis to locate abandoned property that should have been turned over to the state.

Escheatment Defined

Unclaimed property *is tangible or intangible property owed to a person or entity (the owner), yet held by another (the holder).* Generally speaking, under unclaimed property laws (historically referred to as laws of escheat or unclaimed money laws), a holder of unclaimed property that is not ultimately returned to its owner must report and remit that property to the proper state after a designated period of time, referred to as the dormancy period, which varies depending on the type of property involved. A holder that fails to perform these required duties can incur significant liability for the base unclaimed property amount and applicable interest and penalties.

Businesses and residents abandon over a billion dollars of tangible and intangible property annually. Every state has legislation that requires companies to escheat to the state after some period. California, for example, requires escheatment to the state after three years of abandonment. Escheatment includes all forms of property, both tangible and intangible.

For the credit professional, an account's credit balance may qualify as an abandonment of property. Escheatment laws provide that the state becomes the legal owner of abandoned property, based on the concept of state sovereignty. In looking at escheatment as a revenue source, states are considering those businesses that have failed to escheat.

Comprehension Check
Define **unclaimed property.**

Development of Escheatment Law

The history and background of unclaimed property goes back to 1066, the year William the Conqueror combined the best of Anglo-Saxon law with Norman law into English common law. In English common law there is the concept of **escheatment,** *which provided for the reversion of lands to the lord or to the crown upon the failure of capable heirs inheriting under the original grant.* The concept of escheat is referred to in the Magna Carta, written in 1215, and is considered to be the first step in a long historical process leading to the rule of constitutional law. Today, all laws are at the state level because the framers of the Constitution did not reserve the concept of escheat to the federal government. Under the reservation clause of the U.S. Constitution, all powers not granted to the federal government devolve to the states.

Uniform Disposition of Unclaimed Property Act

With the growing popularity of state unclaimed property statutes as a new source of state revenue in the 1950s, uniformity of such laws became a necessity, as controversies between states over conflicting claims to property developed. For example, if a corporation abandons credits it has based on a trade relationship with a vendor, several states might attempt to claim custody. The credits could be covered under the law of the state where the com-

pany was incorporated, or the state where the corporate headquarters was located. In addition, any state that was doing significant business with the corporation might claim the property.

In 1954, **The Uniform Disposition of Unclaimed Property Act (the Uniform Act)** *was introduced to unify the state statutory scheme of escheatment.* The Uniform Act was amended in 1966 and 1981. The Uniform Act attempts to prevent multiple state claims for property by designating the last known address of the owner as the basic test of jurisdiction. Under the Uniform Act, if two states claim the same property, the law of the state of the last-known address of the owner governs. If property is abandoned, the state must establish its right to the property by proving that the property is located within its territorial limits.

Generally, if the property is considered to have a situs, or the place to which, for purposes of legal jurisdiction or taxation, it is subject to escheat. The Uniform Act establishes a period for a presumption of abandonment for most types of property.

Every U.S. state, District of Columbia, Puerto Rico, the U.S. Virgin Islands and Quebec, British Columbia and Alberta in Canada have unclaimed property programs that actively and continuously find owners of lost and forgotten assets. Delaware receives a significant portion of escheated property, notwithstanding that its population is but 800,000. This is because a large percentage of corporations incorporate in Delaware. Under the escheat laws, a party forwards the abandoned property to the company's state of incorporation when the address of the owner can no longer be located.

Business-to-Business Exemption

While the concept of a business-to-business (B2B) exemption to unclaimed property reporting seems simple on its face, the intricacies of state-specific laws greatly complicate the matter. B2B exemptions can vary from a near complete exemption from reporting any property held in the ordinary course of business to a mere deferral of reporting until an ongoing business relationship ceases to exist. Some states take the position that businesses, unlike individuals, do not need the protections afforded by unclaimed property laws. States with B2B exemptions feel that businesses have the capability to ensure their property interests are secured and that taxpayer dollars should not be exhausted to protect these property interests. States with B2B exemptions choose not to interfere with business relationships and instead allow businesses to settle their contractual rights between each other.

Other states have more holder-friendly B2B exemptions, under which property held in the ordinary course of business is exempt from reporting, notwithstanding a lack of an ongoing business relationship with the owner. While holders are still required to attempt to return the property to the owners through due diligence procedures, any unreturnable property becomes the property of the holder.

Not all of these "ordinary-course-of-business" states provide the same breadth of exempt property under their B2B exemption. States such as Indiana, Iowa, Massachusetts, Michigan, North Carolina, and Wisconsin, only exempt credit balances from unclaimed property reporting, but still require the escheatment of uncashed checks and other types of property acquired in the ordinary course of business. Illinois, Kansas, Maryland, Ohio, and Virginia, on the other hand, have broad exemptions that cover most property held in the ordinary course of business and owned by another business, including credit balances and uncashed checks. These states are seen as the most business friendly with reference to their unclaimed property laws. Populous states are pushing for the location of the company's headquarters as the basis for jurisdiction for escheatment.

Risks of Not Escheating

Most states require businesses to review their records to determine whether any property has been unclaimed for the dormancy period and to make an annual report, especially post-September 11. State escheat statutes have harsh provisions for parties that fail to timely report or turn over unclaimed property. In addition to interest that runs from the period that the property should have been turned over, a state may assess fines, penalties and damages.

Escheatment Audit

A state generally enforces its escheatment law through an audit. Audits are generally handled by the state treasurer's office or controller. The scope of the audit can go back several years. The auditors typically request the following:

- Chart of accounts;
- General ledger/trial balance;
- Annual report;
- Journal entries;
- Bank reconciliations; and
- Accounting policies.

Steps to Protect Against Escheatment Claims

A credit executive should develop a game plan, and consider the following:

Step One: Determine the Situation

- Review past compliance. Has the company ever reported unclaimed property? If so, what, when and where?
- Has the company ever been subject to an escheatment audit? If so, what were the results?
- Are there any subsidiaries to be included? Has the company made any recent acquisitions that should be included?

Step Two: Determine Eligible Property

Does the vendor's company have some of the property types covered by most states? For the credit professional, these include:

- Vendor checks.
- Payroll checks.
- Customer credits.
- Refunds.

What states are represented among the names and addresses to be reported? If this is an initial filing, what about years that may not be on the books?

Step Three: Perform the Due Diligence

What due diligence is required by state? It is important to focus on:

- The minimum dollar amount,
- Timing, method, and
- Content notice.

What about operational due diligence? This might include developing a strategy to minimize unclaimed property liability and reviewing potentially reportable items. A due diligence letter should be prepared and include:

- Response deadline.
- Identification number and amount.
- Property type/reason.
- Instructions for claiming.

Step Four: Prepare Reports and Remittances

- Identify due dates for states.
- Prepare a cover sheet with signature.
- Use the proper media, paper, disk, etc.
- Use the proper report format.
- Include the remittance, which might be a check, wire transfer, etc.

Step Five: Filing Reports and Remittances

- File on time to avoid penalties and interest.
- If an extension is received, get it in writing. Only some states will grant them.

Step Six: Follow up and Reconcilement

- Reconcile general ledger to detail.
- Reconcile paid items to appropriate accounts/divisions.
- File any necessary holder reimbursement claims with the states.
- Establish a filing system for reports and work papers.

Credit professionals can also look to the following web site for guidance: National Association of Unclaimed Property Administrators: www.unclaimed.org.

Comprehension Check

If a holder determines it has unclaimed property, what due diligence is required?

Turning Over the Property

If the vendor's company decides to turn over the property to the state, most state statutes provide that the vendor should turn the property over to the state controller. Most legislation requires the vendor to make reasonable efforts to notify the owner of the property by mail that the owner's property will escheat to the state. The notice should be mailed not less than six months before the property is to be turned over to the state controller.

Depending upon the nature, all unclaimed property should either be delivered to the State Treasurer or Controller. When the unclaimed property is cash, delivery is made to the State Treasury; all other types of personal property go to the Controller. The party delivering the property is relieved and held harmless by the state from all claims regarding the property. No action or lawsuit may be maintained against the holder of the property.

Prior to delivery, the holder must furnish notice to the Controller. At a minimum, the notice must include the amount of cash, or nature or description of other personal property; the name and last known address of the person entitled to the property; and reference to a specific statutory provision under which the property is being transmitted.

Comprehension Check

Why is it important to properly report and remit unclaimed property?

POINTS TO CONSIDER

States require all unclaimed/abandoned amounts to be reported, regardless of dollar amount. It is these small amounts that have the greatest likelihood of going unclaimed. Unless a company can refute the presumption of abandonment by documenting that the credit resulted from internal arithmetic errors in invoicing, posting payments and issuing credits, the states can and will make a claim for these credit balances. These items will be used as a basis for creating a statistical sampling, which will likely be extrapolated back over several years.

Most of the states have a due diligence requirement for items over $50. In other words, letters should be sent for all amounts over $50. States (especially Delaware) expect to see a "positive confirmation" from the owner/customer stating that the credit is not due before the amount is considered not to be unclaimed. In the absence of a positive confirmation, the states can make a claim for these credit balances written off.

Some states require the letter to specify the amount outstanding, versus only the account number.

Sarbanes-Oxley Act of 2002

With so many cases of fraud-ridden bankruptcies brought into public view in the beginning of this century, Congress found it necessary to enact **The Sarbanes-Oxley Act of 2002 (SOX).** There is no doubt that the Enron and WorldCom bankruptcies had the most influence in the ultimate passage of this Act: *The SOX was created and enacted to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws and for other purposes.* The sweeping reforms in the Sarbanes-Oxley Act address nearly every aspect and actor in our nation's capital markets.

SOX affects every reporting company, both domestic and foreign, as well as their officers and directors. The Act also affects those that play a role in ensuring the integrity of U.S. capital markets, such as accounting firms, research analysts and attorneys. The over-arching goals of the Act are far-reaching and include restoring investor confidence and assuring the integrity of United States. Within these goals, the principal objectives addressed in the Act can be grouped into the following themes:

- To strengthen and restore confidence in the accounting profession;
- To strengthen enforcement of the federal securities laws;
- To improve the "tone at the top" and executive responsibility;
- To improve disclosure and financial reporting; and
- To improve the performance of "gatekeepers."

The Act comprises 11 titles; what follows is a very broad discussion of this Act and how it pertains to credit. NACM's *Manual of Credit & Commercial Laws* contains a more in-depth presentation of the Act. The 11 titles are:

Title I: Public Company Accounting Oversight Board which provides for the establishment of a Public Company Accounting Oversight Board (the "Board"). As the watchdog for public companies, its intended result is informative, accurate and independent audit reports.

Title II: Auditor Independence prohibits any registered public accounting firm (and any person associated with that firm) to provide any non-audit related services.

Title III: Corporate Responsibility places the burden for proper audit procedures and financial reporting squarely on the shoulders of the principal executive officer or officers and the principal financial officer or officers or other persons performing the duties normally performed by such officers.

The Section 302 Certification can be broken down into three distinct parts:

1. Accuracy and fair presentation of the report's disclosure,
2. Establishment and maintenance of disclosure controls and procedures, and
3. Reporting of deficiencies in, and changes to, internal accounting controls.

A CEO and CFO must certify in any quarterly or annual report, including amendments to such reports that:

- They have reviewed the report;
- Based on their knowledge, the report does not contain any untrue statement of fact or omit a material fact to make the statements not misleading with respect to the period covered by the report; and
- Based on their knowledge, the financial statements, and other financial information included in the report (including, financial statements, footnotes to the financial statements, selected financial data, management's discussion and analysis of operations and financial condition and other financial information in the report), fairly present, in all material respects, the financial condition, results of operations and cash flows of the company as of, and for, the periods presented in the report.

Title IV: Enhanced Financial Disclosures requires financial reports to be prepared in accordance with generally accepted accounting principles (GAAP). This section addresses Management Assessment of Internal Controls.

Title V: Analyst Conflicts of Interest is an amendment to the Securities Exchange Act of 1934 requiring any stock or securities analyst, broker or dealer who has participated or is to participate in a public offering of securities disclose any conflict of interest that is known or should have been known at the time of any public appearance of its report.

Title VI: Commission Resources and Authority authorizes the Commission to carry out its duties and responsibilities.

Title VII: Studies and Reports directs the Comptroller General of the United States to identify factors that have led to the consolidation of public accounting firms since 1989 and the impact, present and future, of such consolidations on capital formation and securities markets.

Title VIII: Corporate and Criminal Fraud Accountability governs the criminal penalties for the destruction, alteration or falsification of records in federal investigations and bankruptcy. Section 806 of this Title is commonly known as the "whistle blower" section.

Title IX: White-Collar Crime Penalty Enhancements provides for penalties for attempts or conspiracy to commit fraud, mail fraud, wire fraud and violations of the Employment Retirement Income Security Act (ERISA) of 1974. Title IX can affect the credit department since the credit manager must certify the accuracy of the accounts receivable asset. This asset is reflected on the balance sheet and all financial reports certified by top management of the company. Failure to accurately certify this asset can result in penalties, fines and possibly imprisonment.

Title X: Corporate Tax Returns states that the corporate tax return should be signed by the chief executive officer of said corporation.

Title XI: Corporate Fraud Accountability establishes fines, penalties and imprisonment for destroying or altering records or impairs, or attempts to alter or impair, the integrity or availability of documents or records for use in official proceedings.

While SOX has received praise for increasing investor confidence in financial statements, SOX-related tasks have also resulted in internal control requirements that have filtered down to credit managers.

To ensure that financial statements are reliable, Section 404 of SOX mandates that rules for establishing responsibility be developed. Section 404 mandates that companies evaluate the effectiveness of their internal controls by having their certifying officers consider two basic questions:

1. Do the employees of the company understand what they need to do to properly prepare external financial reports?
2. What information do the company officers need to make sure their employees have complied?

Three steps can help address these two questions:

Step 1: Identify financial reporting risks and the controls that address them.

Step 2: Ensure that the controls work in practice.

Step 3: Report the conclusions on overall effectiveness and deficiencies.

Credit managers may be asked to sign off on documentation about accounts receivable and credit risk.

Auditors require that there should not be any misstatement of material facts. Credit managers should not let slip by anything that does not seem to be right about the way in which credit and receivables are being reported. SOX affords protections to someone willing to report wrongdoing. Record keeping is an important safeguard to support SOX enforcement. Important documentation to retain include credit applications, loan documents, analyses, financial data and copies of communications such as memoranda, letters and emails.

The SEC recommends that documents be retained for seven years. Its website (www.sec.gov/spotlight/sarbanes-oxley.htm) furnishes pertinent details concerning SOX.

Comprehension Check
Why did Congress enact the **Sarbanes-Oxley Act of 2002?**

Red Flags

Identity theft and the protection of customer information has become an increasingly vital issue for businesses in recent years. The U.S. government has acted swiftly in the face of massive private information heists perpetrated by hackers that have put millions of customers' proprietary information at risk and have severely damaged the reputations of corporations.

In November 2007, a number of regulations that required financial institutions and creditors to develop and implement identity theft programs under the Fair and Accurate Credit Transactions Act (FACTA) were adopted by several federal agencies. In 2008, Sections 114 and 315 of FACT Act, referred to as the Red Flags Rule, went into effect.

Before presenting a discussion of the Red Flags Rule, it is important to note that the Federal Trade Commission (FTC) offered guidance on the extent to which the Red Flags Rule applies to business-to-business transactions involving trade creditors.

The process of determining whether or not a trade creditor has to comply with the Rule requires two steps: a trade creditor must determine whether or not it falls into the definition of being a creditor and second, if it is a creditor, it must then determine whether it has covered accounts that are subject to reasonably foreseeable risk of identity theft.

The Red Flag Program Clarification Act of 2010 limits the applicability of the Red Flags Rule to a creditor, as defined in the Equal Credit Opportunity Act (ECOA), that regularly and in the ordinary course of business:

1. Obtains or uses consumer reports in connection with a credit transaction;
2. Furnishes information to consumer reporting agencies in connection with a credit transaction; or
3. Advances funds to or on behalf of a person based on that person's obligation to repay the funds or repayable from specific property pledged by or on behalf of that person.

The term, advances funds, refers to money, rather than goods or services, narrowing this remaining category of creditor only to entities making loans. If a trade creditor does not meet the definition of creditor because, for example, it only deals with established corporate entities and does not rely on personal consumer credit reports or furnish information to consumer reporting agencies or make loans, then the Rule does not apply.

A trade creditor that does not fall into any one of these categories does not meet the definition of a creditor under the Red Flags Rule. Should a trade creditor regularly obtain and rely on an individual credit report in making credit decisions, whether the report is on the principal of a small business or a personal guarantor or a non-corporate entity like a mom-and-pop store or sole proprietorship, then the trade creditor is subject to the "Red Flags" Rule, meaning that, if it has covered accounts based on an analysis of its risk level, it must create its own written program for fighting identity theft.

Ultimately, if a company sells on a purely business-to-business basis, and does not fall into any of the defined categories of creditor, then it does not have to comply with the Red Flags Rule.

The Red Flags Regulations and Guidelines require most creditors and financial institutions to adopt a written program to detect, prevent and mitigate identity theft in connection with the new opening of a covered account or any existing covered account. Every creditor and financial institution covered by the rule must adopt a risk-based program that identifies red flags relevant to its own operation and, more importantly, how it will respond to them. The responsibility for rulemaking and enforcement was transferred to the U.S. Securities and Exchange Commission and the U.S. Commodity Futures Trading Commission.

Part I: Risk Assessment to Identify Relevant Red Flags

Red Flags *are any pattern, practice or specific activity that indicates the possible risk of identity theft; companies need to identify the Red Flags specific to it by identifying the types of accounts offered or maintained.* An important key to the Red Flags program is for every company to examine the methods by which it permits accounts to be opened along with its previous experience with identity theft.

Are documents, such as state- or government-issued forms of identification, presented during transactions? If so, what steps are taken to check for document alterations or forgeries? How is consistency in presented documents checked; does the person presenting match the documents? Is there a foreseeable risk of identity theft in connection with business accounts that may be opened or accessed remotely, through methods not requiring face-to-face contact such as the Internet or over the phone? How is a change of address monitored? For example, what if an increased line of credit is requested, or additional authorized account users are requested, immediately following a change of address notice? How is the identity of the purchaser verified on orders received via purchase order?

More and more, business is being done electronically, with companies offering access to accounts via the Internet or over the telephone. The Federal Bureau of Investigation's Cyber Division recently announced that crimes against U.S. businesses are increasing and that cyber criminals are becoming more brazen and effective at stealing financial information and perpetrating identity theft crimes.

The case of WESCO Distribution, discussed in the Fraud Chapter, highlights weaknesses in the trade credit industry. Criminals have posed as executives of various major corporations to pilfer hundreds of thousands of dollars of merchandise from unsuspecting companies by preying on salespeople eager to make or exceed sales targets. WESCO's Asset Protection Manager William Coe developed his own set of "red flags" that were distributed regularly to sales team members to prevent needless losses.

Coe understood that WESCO's identity was being used to defraud others and realized it was only a matter of time before criminals posing as another company would try and victimize WESCO. It wasn't long before WESCO staff caught fraudulent purchase orders being sent to them from individuals posing as major companies and customers of the distributor.

WESCO uses the following set of "red flags" when considering purchase orders or applications:

- The sender's email uses a generic service rather than a company name.
- Large quantities of the same item are ordered.
- The shipping address given differs from the company's address or is a new location for the customer.
- The language used in the emails is flawed, consistently misspelled and reads like it's from a foreign translation.
- Multiple credit cards are used for the purchase.
- The purchaser attempts to get net 30 terms.
- An alternative shipping method, faster than typical, is requested such as overnight air or rush pick-up.
- Multiple rush orders are received from the same company in a short period of time.

These factors are strikingly similar to several of the Red Flags identified by the FTC and provide a great starting point for all trade creditors in their efforts to prevent fraud. For example, in the case of fraudulent purchase orders sent to companies under the guise of WESCO, the purchase orders displayed a residential address not affiliated with the company and the phone numbers listed were incorrect or disconnected. Unfortunately, the salespeople and credit managers involved didn't further investigate the suspicious information. They rushed the shipments out the door and thousands upon thousands of dollars in merchandise were lost. WESCO ultimately had to send out alerts to all of the companies with which it does business about the theft of WESCO's identity and stated that if any company has the slightest bit of doubt about a purchase order received from WESCO, to please contact them.

Rush orders from new accounts may merit further checking. Many fraudulently placed rush orders are made citing holiday or seasonable demand. Generally speaking, sales teams have to work to solicit new business; when it happens the other way around and orders arrive too easily, it's a Red Flag that merits further investigation and verification.

Small initial orders from new customers, or from older customers under new management, may also be Red Flags. Most credit professionals would not consider approving a substantial order from a new customer without verifying its credit history and references; and yet, on small orders, overworked and understaffed credit depart-

ments may only conduct a cursory check on a new customer placing a small order. Conversely, large orders are often a Red Flag. It is a best practice in the commercial credit arena to check on why a large order is merited or needed.

Another Red Flag could be an answering service that offers to have a reference call back or, worse, a reference that provides an immediate, glowing report on an applicant—without ever having to look up records. An unusually large number of inquiries from other suppliers regarding a new account may be a Red Flag, signaling that the debtor is placing an extraordinary amount of orders.

If a company conducts counter sales, both corporate and personal checks may be a source for detecting Red Flags. As part of its check guarantee program, NACM Business Partner United Tranzactions (UTA) requires that company names be imprinted on corporate checks (no temporary checks) in addition to an address. While post office box numbers may appear on the check, a physical address must be requested and noted on all corporate checks. UTA also requires that a telephone number be recorded on the check, if it is not imprinted, in order for a check to be eligible for its check guarantee program. When inspecting personal checks, UTA requires the check writer's name to be imprinted on the check (no temporary checks), that a physical address be recorded on the face of the check in handwriting if only a post office box address is imprinted, and that a home telephone number be recorded. Identification is required and the signature must match the pre-printed name on the check.

Part II: Detecting Red Flags

Once the Red Flags that are relevant to a business are identified, policies and procedures must be established to detect them in day-to-day operations. For example, a Red Flag may be spotted when an order originating with the sender using a generic email account or when a new "ship to" address is verified. Red Flags can be indentified during a risk assessment when customers are authenticated, transactions are monitored or requests for address changes are verified. A description of what a company will do when a Red Flag is spotted should be included in a company's program. Some Red Flags may seem harmless on their own, but they can signal identity theft when paired with other events, such as a change of address coupled with the use of an address associated with fraudulent accounts.

Part III: Respond Appropriately to Any Red Flags Detected to Prevent and Mitigate Identity Theft

A written program policy provides for appropriate responses to the detected Red Flags to mitigate identity theft of a person or a company. Companies should consider factors that may heighten the risk of identity theft, such as a data security breach that resulted in unauthorized access to a customer's account records.

Once fraudulent activity is detected, credit department personnel must act quickly to protect customers and the company itself from loss and damage. Document the facts and findings supporting the conclusion that the transaction is fraudulent or authentic. As always, the proper protocol must be followed in presenting a written summary of the situation to management.

Part IV: Update the Written Program Periodically to Reflect Changes in Risks to Customers or to Business from Identity Theft

No matter how good a program looks on paper, the true test will lie in how well it works. It should include a description of how it will be administered covering topics such as how company management will maintain the program and keep it current on an ongoing basis. How a company will train staff to recognize the Red Flags and follow through with appropriate actions based on its program is described in this part. The program will also need to describe how a company will oversee service providers to ensure that their actions comply with these Red Flags Regulations and its Red Flags program. It is critically important to review and update a written Red Flags program to reflect changes in risks to customers or to the company from identity theft.

Should a company begin to experience higher incidences of fraud, it may be appropriate to change its methods of verifying the identity of customers. If new types of accounts are offered, the program will need to be updated

accordingly. Any changes in a business such as a merger, acquisition, joint venture or changes in service provider arrangements need a program review.

Part V: Oversight of This Program

The FTC mandates that there be oversight of a company's Red Flags program by their board of directors, a committee of the board of directors or designated senior management. The oversight includes the assignment of the specific responsibility for the program's implementation, including the review of reports prepared by staff regarding compliance, and the approval of material changes to the program as necessary to address changing identity theft risks.

Companies will need to issue an annual report which discusses the effectiveness of its program and procedures, significant incidents involving identity theft and management's response and recommendations for changes to the program. Management is responsible for ensuring that any deficiencies raised within the annual report are addressed.

Penalties for Failure to Comply with the Red Flags Regulations

Many financial institutions covered by the Red Flags Regulations are subject to oversight by the appropriate federal banking regulators, which may impose penalties consistent with their regulatory authority.

Creditors who fall under these rules are regulated by the FTC. In the event of a known violation, which constitutes a pattern or practice of violations, the FTC may commence a civil action to recover a civil penalty in a federal district court. Penalties imposed by the FTC for violations of FACTA (Fair and Accurate Credit Transaction Act of 2003) may not exceed $3,500 per infraction.

In addition to regulatory enforcement actions, users of consumer reports who fail to comply with the address discrepancy regulations are subject to civil liability under §§ 616 and 617 of the Fair Credit Reporting Act.

Comprehension Check
What is the **Red Rlags rule?**

Figure 6-1 Sample Policy for Red Flag Rules

Please note that the following sample policy suggests likely situations that may indicate possible identity theft fraud. Each company must conduct its own risk assessment and customize how it will respond as Red Flags are discovered.

[Insert Company Name] Identity Theft (Red Flags) Program

PROGRAM INTRODUCTION

This **RED FLAGS** program is designed to provide protocols and guidelines for the detection, prevention and mitigation of identity theft in connection with the opening of a covered account or any existing covered account. In preparing this program, [company name] has striven to identify patterns, practices and specific forms of activities, or Red Flags, that could indicate the possible existence of identity theft. This program better positions [company name] to stop identity theft at its inception. This program also serves as a testament to [company name]'s compliance with the FTC's Red Flags Regulations.

This program incorporates existing policies, procedures and other arrangements that control reasonably foreseeable risks to [company name]'s customers or reasonably foreseeable risks to the safety and soundness of [company name] from identity theft.

Throughout this policy, the term "covered account" means an account that [company name] offers or maintains—primarily for personal, family or household purposes—or that involves or is designed to permit multiple payments or transactions. A "covered account" is any other account that [company name] offers or maintains for which there is a foreseeable risk to customers or to the safety and soundness of [company name] from identity theft, including financial, operational, compliance, reputation or litigation risks.

The term "identity theft" means a fraud committed or attempted using the identifying information of another person without authority.

"Identifying information" means any name or number that may be used alone or in conjunction with any other information to identify a specific person, including any:

1. Name, Social Security number, date of birth, official state- or government-issued driver's license or identification number, alien registration number, government passport number, or employer or taxpayer identification number;
2. Unique biometric data, such as fingerprint, voiceprint, retina or iris image, or other unique physical representation;
3. Unique electronic identification number, address or routing code; or
4. Telecommunication identifying information or access device (as defined in 18 U.S.C. 1029(e)).

SECTION I: RISK ASSESSMENT/IDENTIFYING RELEVANT RED FLAGS

(Please note that these possible risk factors are merely suggestions; your company will need to identify its Red Flags based on its business, its customers, etc.)

[Insert company name] has considered the following factors in identifying relevant Red Flags for covered accounts:

Customize the possible risk factors listing:

1. The types of covered accounts your company offers or maintains
2. The methods your company provides to open its covered accounts (written application, verbal/over the phone, verbal/physical call by sales, online/Internet). Effective security management requires your company to deter, detect and defend against security breaches. That means taking reasonable steps to prevent attacks,

Figure 6-1 Sample Policy for Red Flag Rules continued

quickly diagnosing a security incident and having a plan in place for responding effectively.

3. The methods your company provides to access its covered accounts and
4. Your company's previous experiences with identity theft.

Customize the types of things that are Red Flags signaling the possibility of corporate identity theft:

1. The sender's email uses a generic service rather than a company name when placing an order
2. Large quantities of the same item are ordered; an unusual increase in the volume ordered by an existing customer
3. The shipping address given differs from the company's address or is a new location for the customer
4. Personal or common carrier pick-up of the goods ordered
5. An alternative shipping method, faster than typical mail, is requested such as Overnight Air
6. The language used in the emails is flawed, consistently misspelled and reads like it's from a foreign translation
7. Multiple credit cards are used for the purchase
8. The purchaser attempts to get net 30 terms
9. Multiple rush orders are received from the same company in a short period of time
10. The credit references are provided verbally and only telephone numbers for the references are provided (no physical address information)
11. The phone number of the credit reference can't be verified
12. The name of the business placing the order is confusingly similar to another well-known, successful business
13. Inability to reach the principals of the business
14. The order is placed by a business that had a recent change in ownership; the ownership change was not well-communicated or was downplayed

Customize notifications or warnings from a consumer reporting agency that constitute Red Flags:

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

Figure 6-1 Sample Policy for Red Flag Rules continued

Customize suspicious documents presented to your company that are Red Flags:

1. Documents provided for identification appear to have been altered or forged.
2. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the information.
3. Other information on the identification is not consistent with readily accessible information that is on file with your company, such as a signature card or a recent check.
4. An application appears to have been altered or forged, or gives the appearance of having been destroyed or reassembled.

Customize suspicious personal identifying information:

1. 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.
2. 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.
3. 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;
   B. The phone number on an application is the same as the number provided on a fraudulent application.
4. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by your company. 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.
5. The SSN provided is the same as that submitted by other persons opening an account or other customers.
6. 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.
7. 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.
8. Personal identifying information provided is not consistent with personal identifying information that is on file with your company.

Figure 6-1 Sample Policy for Red Flag Rules continued

Customize the unusual use of, or suspicious activity related to, your company's covered accounts:

1. 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, for the addition of authorized users on the account.
2. A new revolving credit account is used in a manner commonly associated with known patterns of frauds. For example:
   A. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (electronics equipment or jewelry)
   B. The customer fails to make the first payment or makes an initial payment but no subsequent payments
3. 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 where 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 funds transfer patterns in connection with a deposit account;
   E. A material change in telephone call patterns in connection with a cellular phone account.
4. 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.
5. The credit report reveals that all accounts are newly/recently opened and provides little or no historical credit information or payment trends.
6. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
7. Your company is notified by the customer that he/she is not receiving paper account statements.
8. Your company is notified of unauthorized charges or transactions in connection with a customer's covered account.
9. Your company is notified by the 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.

Additional Options to Include in Your Company's Program

Your company's commitment to securing sensitive customer information:

1. Safeguarding sensitive data in your files and on your computers is just plain good business. After all, if that information falls into the wrong hands, it can lead to fraud or identity theft. A sound data security plan is built on five key principles:
   A. Know what personal information you have in your files and on your computers.
   B. State your company's policy on document retention.
   C. How is sensitive information protected while in the care of employees?

Figure 6-1 Sample Policy for Red Flag Rules continued

D. How is sensitive information properly disposed of?
E. Should there be a breach to sensitive data, state your company's response plan.

2. Does your company have a records retention manager to supervise the disposal of records containing customer information? If you hire an outside disposal company, conduct due diligence beforehand by checking references or requiring that the company be certified by a recognized industry group.
3. Discuss how information is disposed of; documents containing sensitive information should be burned, pulverized, or shredded so that the information cannot be read or reconstructed.
4. Discuss how computers, disks, CDs, magnetic tapes, hard drives, laptops, PDAs, cell phones, or any other electronic media or hardware containing customer information are destroyed, discarded or erased.

SECTION II: DETECTING THE RED FLAGS

For each instance identified in Section I, explain how your company will take action.

For example, since your company has identified that when an order is received by email and the sender used a generic service rather than a company-issued email account, credit department staff will verify the order by contacting the company through known contacts or will research contact information independently and research the order.

Since your company has identified that the shipping address supplied for an order differs from the company's address or is a new location for the customer, the credit department staff will verify the order by contacting the company through known contacts to verify the order.

SECTION III: RESPOND APPROPRIATELY TO ANY RED FLAGS DETECTED TO PREVENT AND MITIGATE IDENTITY THEFT

If fraudulent activity is detected, [insert company name] will act quickly to protect customers from loss and damage. Our employees will document the facts and findings in writing, supporting their conclusion that the transaction is fraudulent or authentic. The report will be presented to [insert who is to receive the report].

Customize the appropriate responses your company will make:

1. Monitoring a covered account for evidence of identity theft
2. Contacting the customer
3. Changing any passwords or security codes that permit access to a covered account
4. Reopen a covered account with a new account number
5. Not opening the account
6. Closing the account
7. Not attempting to collect on a covered account or not turning a covered account over to a third party collection agency
8. Notifying law enforcement
9. Determining that no response is warranted under the particular circumstances

Figure 6-1 Sample Policy for Red Flag Rules continued

SECTION IV: PERIODIC REVIEW OF THE WRITTEN POLICY TO REFLECT CHANGES IN RISKS TO CUSTOMERS OR TO BUSINESS FROM IDENTITY THEFT

[Insert company name] will update this policy [insert frequency (annually, semi-annually, quarterly)] to reflect changes in risks to customers or to [insert company name]'s safety and soundness from identity theft based on factors such as:

Customize the factors relevant to your company:

1. The experiences of your company with identity theft
2. Changes in methods of identity theft
3. Changes in methods to detect, prevent and mitigate identity theft
4. Changes in the types of accounts that your company offers or maintains
5. Changes in the business arrangements of your company, including mergers, acquisitions, alliances, joint ventures and service provider arrangements.

SECTION V: OVERSIGHT OF THIS PROGRAM

Oversight of this program will be the responsibility of [insert appropriate management official, committee, Board of Directors], which includes the responsibility and accountability for the program's implementation and the review of reports prepared by staff regarding compliance with this program.

An annual report discussing the effectiveness of the program and procedures, significant incidents involving identity theft and management's response and recommendations for changes to the program will be issued by [insert date].

Key Terms and Concepts

Adverse action as defined by the ECOA, 6-11
- reduction of credit availability on an existing account, 6-11
- refusal to grant credit, 6-11
- refusal to increase credit, 6-11
- termination of credit on an existing account, 6-11

Antitrust Procedures and Penalties Act, 6-6
Clayton Act of 1914, 6-3–6-4
Consumer Financial Protection Bureau, 6-13
Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, 6-13–6-14
Electronic signature, 6-17, 6-18
Electronic Signatures in Global and National Commerce Act (E-Sign Act), 6-17–6-18
Equal Credit Opportunity Act and Regulation B, 6-8–6-13
Escheatment, 6-19–6-22
Factoring, 6-9
Fair Credit Billing Act, 6-16–6-17
Fair Credit Reporting Act (FCRA), 6-6–6-8
Fair Debt Collection Practices Act (FDCPA), 6-14–6-15
Federal Trade Commission Act of 1914, 6-4
1976 Antitrust Act, 6-6
Price-fixing, 6-5
Red Flags, 6-25–6-34
Robinson-Patman Act of 1936, 6-4–6-5
Sarbanes-Oxley Act (SOX), 6-23–6-24
Sherman Act of 1890, 6-2
Trade credit, 6-9
Truth in Lending Act and Regulation Z, 6-15– 6-16
Unclaimed property, 6-19–6-22
Uniform Disposition of Unclaimed Property Act, 6-19–6-20
Usury, laws of, 6-16
Venture capital, 6-9
Working capital, 6-9

Comprehension Check

1. What is the purpose of **U.S. antitrust law?**
2. What is the **Sherman Act** designed to prevent?
3. What does the **Robinson-Patman Act** specifically forbid?
4. What types of business practices does the term **price discrimination** include?
5. What is the purpose of the **Fair Credit Reporting Act?**
6. What is the purpose of the **Equal Credit Opportunity Act?**
7. The ECOA defines the term **adverse action.** List the four types of action that qualify as adverse under the ECOA.
8. What is the purpose of the **Dodd-Frank Wall Street Reform Act?**
9. How does the **Fair Debt Collection Practices Act** affect the collection of a debt by a debt collector?
10. What is the purpose of the **Truth in Lending Act?**
11. List two provisions of the **E-Sign Act.**
12. What are some advantages of **e-signatures?**
13. Define **unclaimed property**.
14. If a holder determines it has unclaimed property, what due diligence is required?
15. Why is it important to properly report and remit unclaimed property?
16. Why did Congress enact the **Sarbanes-Oxley Act** of 2002?
17. What is the **Red Flags rule?**

Summary

- Understanding the legal environment surrounding business on national and state levels is critical to a credit professional's role. Legislation protects the rights of creditors as well as poses limitations to business activity. Penalties and criminal action that may be filed against individual credit professionals and the business if conduct is found to be outside the boundaries of the law.
- Antitrust regulation was enacted at the turn of the 20th century to mitigate the effect of powerful monopolies on small businesses. The four major federal acts combating monopolies include:
  - **The Sherman Act**
  - **The Clayton Act**
  - **The Robinson-Patman Act**
  - **The Federal Trade Commission Act**
- The **Sherman Act** was designed to prevent monopolies and unfair restraints of trade. Although it does not prohibit all restraints of trade, it does outlaw contracts, combinations, or conspiracy to restrain trade, and monopolization that is deemed unreasonable.
- The **Clayton Act** was created to correct the shortcomings of the Sherman Act. It gives administrative agencies the power to stop violations of the law before they develop into actuality. The law makes it unlawful to create exclusive dealing arrangements, as well as any deal containing arrangements that involved restricting the sale to or from a competitor. It also restricted companies from obtaining stock of other companies that would considerably lessen the competition in the market place.
- The **Federal Trade Commission Act** is the broadest act and prohibits any act that attempts or is designed to deceive the public.
- The **Robinson-Patman Act** is designed to target direct or indirect price discrimination. This is particularly important to credit professionals, and involves:
  - A different price charged to different purchasers of the same type
  - Differences in terms and conditions of sale
  - Preferential credit terms
  - Credit terms which are an inseparable part of price
- For a person to be found liable for price discrimination there is no need for an arrangement, combination, association or conspiracy. They only need to be engaged in at least two transactions crossing state lines, and for the consumption or resale within the United States.
- Meeting competition is the most common defense against claims of unlawful price discrimination.
- The **Fair Credit Reporting Act (FCRA)** requires consumer credit reporting agencies to adopt reasonable procedures to meet the needs of consumer credit, employment, insurance, and all other information that is fair and equitable to consumers. It concerns credit extended to consumers and not commercial credit transactions. The law states that a credit report may not be initiated or requested without the written consent of the individual and there is a permissible business use defined by statute.
- The **Equal Credit Opportunity Act and Regulation B (ECOA)** was created to promote the availability of credit regardless of one's race, color, religion, national origin, sex, marital status or age.

- With gross revenues of $1 million or less in the preceding fiscal year, the creditor must provide written or oral notice of **adverse action** within 30 days of receiving the application. Adverse actions are:
  - Refusal to grant credit
  - Refusal to increase credit on an existing account
  - Reduction of credit availability on an existing account
  - Termination of credit on an existing account
- A credit hold is not deemed adverse if the account has been slow to pay or is delinquent. If a creditor violates a provision of the **ECOA**, they are liable for actual damages sustained by the applicant. With all costs included, **ECOA** damages can be detrimental.
- Any disclosure can be provided electronically as long as it is clear and the creditor has obtained the applicant's affirmative consent to obtained electronic communication.
- The **Dodd-Frank Wall Street Reform and Consumer Protection Act** establishes a **Consumer Financial Protection Bureau (CFPB),** and has a primary mission to monitor consumer lending. It also requires the disclosure of the principal reasons for denying or taking adverse action against an application for an extension of credit.
- The **Fair Debt Collection Practices Act** was created to make fair laws for the benefit of debtors when creditors attempt to recover debts. The **FDCPA** focus is on the collection activities of third-party collectors. Prohibitions include, but are not limited to, the following:
  - Misrepresenting the character or the amount of a debt
  - Threatening to take action prohibited by law
  - Threatening to take action that is not intended to be taken
  - Making repeated calls for the purpose of harassment
- The **Truth in Lending Act (TILA)** was created with the intention of protecting and educating consumers in the field of purchasing credit. Sellers of credit are mandated by law to disclose certain information when offering credit. This includes information regarding the interest rates, finance charges and fees that will apply when accepting such credit terms.
- **E-Sign Act** was instituted to continue the facilitation of electronic commerce. It is vital to understand that e-signatures may not be denied legal effect, validity, or enforceability solely because they are in electronic form, and just because an electronic signature was used in the creation of a contract relating to a transaction. It is also important to understand that an email can constitute a valid and enforceable agreement.
- E-signatures make business on a domestic and international level faster and more efficient. They benefit both businesses and consumers from a legal standpoint, as well as reduce administrative work associated with printing, signing and rescanning a document in order to send it electronically.
- Due to the need for increased security after the events that took place on September 11th, states have looked for other sources of revenue, which has made escheatment an appealing source of revenue. **Escheatment** is the states right to unclaimed property. Laws differ by state, so it is important for credit professionals to know and understand the laws of escheatment in their particular state or fines, penalties and damages may be taken against a business.
- The **Sarbanes-Oxley Act (SOX)** was instituted to protect investors by improving the accuracy and reliability of corporate disclosures. The overarching goals of the act were to restore investor confidence and assure the integrity of business practices within the United States. The main objectives are to:
  - Strengthen and restore confidence in the accounting profession

  - Strengthen the enforcement of the federal securities law
  - Increase executive responsibility
  - Improve disclosure and financial reporting
- The main components of the act include, but are not limited to, the creation of a **Public Company Accounting Oversight Board PCAOB),** the use of independent auditors, the requirement of executives to be responsible for the accuracy of all public documents, the use of **generally accepted accounting principles (GAAP**), and the disclosure of any known conflict of interest.
- As of November 2007, the **Fair and Accurate Credit Transactions Act (FACTA)** requires financial institutions and credit managers to develop and implement identity theft programs. **Red Flags** are any potential risks that could arise in terms of identity theft.
- As a business, it is important to:
  - Do a risk assessment to identify relevant red flags
  - Detect red flags
  - Respond appropriately to red flags to mitigate risks of identity theft
  - Update the written program periodically to reflect changes in risks to consumers or to business from identity theft
  - Have oversight dedicated to a company's Red Flags program

References and Resources

Borges, Wanda. *Antitrust, Restraint of Trade, and Unfair Competition: Myth vs. Reality.* Columbia, MD: National Association of Credit Management, 1998.

Business Credit. Columbia, MD: National Association of Credit Management. (This 9 issues/year publication is a continuous source of relevant articles and information. Archived articles from *Business Credit* magazine are available through the web-based NACM Resource Library, which is a benefit of NACM membership.)

Business Credit and the Equal Credit Opportunity Act and Regulation B. Columbia, MD: National Association of Credit Management, 2001.

Government resources: The Federal Trade Commission at www.ftc.gov, the Federal Deposit Insurance Agency at www.fdic.gov and the Department of Justice at www.doj.gov.

Manual of Credit and Commercial Laws. Columbia, MD: National Association of Credit Management, current edition.

Miller, Roger and Gaylord Jentz. *Business Law Today.* 5th ed. London: Thomson Learning, 2000. *See* Unit 7.

Shenefield, John H. and Irwin M. Stelzer. *The Antitrust Laws: A Primer,* 4th ed. La Vergne, TN: AEI Press, 2001.