THE RED FLAGS RULES AND YOUR CUSTOMER’S PRIVACY RIGHTS: What Does it Mean to the Credit Professional?

Scott E. Blakeley, Esq.

Blakeley LLP
4685 MacArthur Court, Suite 421
Newport Beach, CA  92660
Tel: 949/260-0612
Fax: 949/260-0613
SEB@BlakeleyLLP.com
www.BlakeleyLLP.com

Los Angeles Office:
515 South Flower Street, 36th Floor
Los Angeles, CA  90071
Tel: 213.382.0675

Scott Blakeley is a partner in the California law firm of Blakeley & Blakeley LLP, where he advises companies around the country regarding creditors’ rights, commercial law, e-commerce and bankruptcy law. He was selected as one of the 50 most influential people in commercial credit by Credit Today. He is contributing editor for NACM’s Credit Manual of Commercial Law, contributing editor for American Bankruptcy Institute’s Manual of Reclamation Laws, and author of A History of Bankruptcy Preference Law, published by ABI. Credit Research Foundation has published his manuals entitled The Credit Professional’s Guide to Bankruptcy, Serving On a Creditors’ Committee and Commencing An Involuntary Bankruptcy Petition. Scott has published dozens of articles and manuals in the area of creditors’ rights, commercial law, e-commerce and bankruptcy in such publications as Business Credit, Managing Credit, Receivables & Collections, Norton’s Bankruptcy Review and the Practicing Law Institute, and speaks frequently to credit industry groups regarding these topics throughout the country. Scott holds a B.S. from Pepperdine University, an M.B.A. from Loyola University and a law degree from Southwestern University. He served as law clerk to Bankruptcy Judge John J. Wilson.
I. Introduction
   
A. Reduce business to business trade credit risk
   
B. FCRA: Fair Credit Reporting Act
   
C. FACTA
   
D. Red Flags Rule

II. Red Flags Rule: An Identity Theft Prevention Program

A. Amends 2003 FACTA
   
B. Difference between data security and the red flags rule

   1. Data security aimed at protecting personal information that you have about customers
   
   2. Red Flags Rules picks up where data security leaves off
      
         a. Stopping and identifying thieves from using someone else's personal info at your business to commit fraud or illegally obtain goods/services
   

C. Why does the FTC keep extending the enforcement of “Red Flags” Rule?

   1. An effort by the FTC to redouble its efforts to educate small businesses and other entities about complying
   
   2. Easing compliance by offering additional resources
   
   3. Clarifying whether businesses are covered
   
   4. Clarify compliance procedures
   
   5. New date: November 1, 2009

D. Who must comply?

   1. Creditors holding covered accounts
      
         a. Covered account
            
           i. Checking and savings accounts
           
           ii. Small business or sole proprietorship accounts
           
           iii. All accounts with “foreseeable risk of identity theft”
      
         b. Extend, renew, or continues credit
THE RED FLAGS RULE

c. Assignee of original creditor
d. Any form of deferred payment qualifies
e. Finance companies

E. Who might not the Red Flags Rules apply to?

1. Accepting credit cards or other forms of payment doesn’t make you a creditor under Red Flags Rule
2. Vendors that require payment before work begins
   a. Red Flags Rule applies to businesses that regularly defer payment until after services have been performed

F. Is your business at low risk for identity theft?

1. Do you know your clients personally?
2. Has your company experienced an incident of identity theft?
3. Are you in a business where identity theft is uncommon?

G. How does it apply to business to business trade credit relationships?

1. No distinction between whether it’s business or consumer credit
   a. Do a risk assessment and assess the interaction you have with your customers
      i. Risk factors: customer credit files with sensitive private information, customer credit card numbers, customer checking account information
   b. Is there enough security to protect your customers from identity theft?
   c. How do customers open or access their accounts?

2. Mandatory identity-theft prevention program

3. Penalties for failure to comply
   a. In the event of a pattern or practice of violations, FTC may commence a civil action to recover a civil penalty in a federal district court
   b. Penalties imposed by the FTC for violations of FACTA may not exceed $3,500 per infraction
   c. Users of consumer reports who fail to comply with the address
THE RED FLAGS RULE

discrepancy regulations subject to civil liability under 616 and 617 of the Fair Credit Reporting act

d. The FTC does not conduct routine compliance audits
e. No private right of action: consumer cannot sue you under the Red Flags Rule

H. Methods to red-flag the red flags

1. FTC’s do-it-yourself template

2. Identification of red flags

   a. Examples

      i. Notice of fraudulent use of an account
      ii. Address discrepancies
      iii. Returned mail on active accounts
      iv. False identification
      v. Documents provided for identification appear to have been altered or forged
      vi. Inconsistent information with what is currently on file
      vii. Application appears to have been altered or forged
      viii. Multiple credit cards used
      ix. SSN verification
      x. Noteworthy changes in spending patterns

3. Detecting red flags

   a. Design a plan to ensure the identifiers aren’t ignored

   b. Examples

      i. Challenge questions
      ii. Authenticating accounts
      iii. Transaction monitors and logs
      iv. Passwords and PIN’s
THE RED FLAGS RULE

v. Create of chain of upward command
vi. Credit card authorization forms required
vii. Verification of references

4. Response to red flags
   a. Examples
      i. Periodic password changes
      ii. Email addresses from non-company urls
      iii. Mailing/shipping addresses that are residences
      iv. Issue new account numbers to existing accounts
      v. Requiring secondary identification
      vi. If identity theft claim is used, require proof
      vii. Freezing goods or services until discrepancy is resolved
      viii. Notification of law enforcement
      ix. No response

5. Program administration and updates
   a. Clearly written
   b. Concise outline of responsibilities
   c. Obtain approval from Board of Directors/a committee of your board/Program manager
   d. Staff training
   e. Outline upward chain of command
   f. Program reviews
   g. Periodic updates
   h. Annual report to Board of directors/senior management level person
   i. Significant events
j. Properly dispose of sensitive information per company’s records retention program
   i. CC Numbers,
   ii. Bank account numbers on credit applications
   iii. Copies of customers’ checks

III. Other Privacy Laws that may Affect the Credit Professional

IV. Model State Privacy Law
   A. Purpose
   B. Key Terms of Model law
      1. Electronic Credit Department
      2. What Information is Covered?
      3. What is a Security Breach?
      4. Must a Company reside in the model state?
   C. Notice Requirement
      1. Model law requires a company give prompt notice to customers after a security breach
   D. Complying with Model Law
   E. Encryption
   F. Security
   G. Written Manual
   H. Training
   I. Credit Application
   J. Personal Guarantee
   K. Privacy Audit
   L. Violation of Model Law

V. Fair Credit Reporting Act
   A. Purpose
B. Credit Reporting and Commercial Credit

C. Legitimate Business Purpose Exception May Not Be Recognized

D. Relevance of Consumer Reports When Commercial Credit Extensions Are Made To A Corporation, LLC or partnership

E. Notification If Credit Is Declined Based Upon Consumer Credit Report

F. Penalties For Violating FCRA

VI. Fact Act

A. The Fact Act Amends the Fair Credit Reporting Act
   1. The seven national uniformity provisions prevent states from creating conflicting legislation concerning the sharing of credit information, credit bureau reports, application information, and transaction and experience data

B. Changes the Credit Professional May Anticipate as a Result of the Fact Act

C. Attempts to Stop the Epidemic of Identity Theft
   1. Collection Agencies and the Fact Act
   2. Proper Disposal of Credit Information

VII. Patriot Act

A. Introduction
   1. On October 26, 2001, Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (the “USA Patriot Act”)
   2. Main purpose to bolster national security after the September 11th attacks
   3. Based on identification of customers and their activities
   4. Promulgates broad, new requirements for both financial and non-financial institutions
   5. Makes significant changes to the Money Laundering Control Act of 1986
   6. Non-Financial Institutions
   7. Financial Institutions
   8. For non-traditional financial institutions, implementing a compliance program will present significant adjustment to operations
   9. Required to share information and provide Suspicious Activity Reports (“SARS”)
VIII. Equal Credit Opportunity Act

A. Purpose: To ensure that grantors of credit are not engaged in discrimination

B. Federal Statute: Applies to all states.

C. Consumer Credit versus Commercial Credit. Consumer legislation that applies to commercial transactions. A vendor may not refuse to grant trade credit or discourage a vendor credit applicant from asking for credit because of sex, marital status or any of the reasons cited above

   1. General Rule. A “creditor” shall not “discriminate against an applicant” on a “prohibited basis” regarding any aspect of a “credit transaction”

   2. Credit. The right granted by a creditor to an applicant to defer payment of a debt, incur debt and defer its payment, or purchase property or services and defer payment

   3. Creditor

   4. Credit transaction - means every aspect of an applicant’s dealings with a credit grantor regarding an application for credit or an existing extension of credit (includes information requirements, investigation procedures, standards of creditworthiness, terms of credit, furnishing of credit information, revocation, alteration, or termination of credit, and collection procedures)

D. Discrimination Actionable Under ECOA

E. Stages of the Credit Transaction Subject to ECOA

F. Company Policy

   1. Written Manual

   2. Training

G. The Credit Application

   1. Disclosures

   2. Guarantors

H. Evaluation of Application

   1. Not Relying on Prohibited Basis

   2. “Completed” Application

   3. Adverse Action

   4. Not Adverse Action
THE RED FLAGS RULE

I. Credit Executive’s Notification of Adverse Action
   1. 30-Day Rule to Notify of Adverse Action
   2. If “adverse action” is taken regarding an application, notice must be provided to the applicant that he/she has the right to request reasons for the adverse action in writing within 60 days of such action. See Exhibit C
   3. Form of Notice
   4. Statutory Notice. ECOA provides that the notice of adverse action must contain language that is substantially similar to the following:
   5. 60-Day Rule for Applicant to Request Reasons for Adverse Action
   6. Responding to Request

J. Credit Executive’s Reply

IX. Confidentiality Agreements
   A. What are Confidentiality Agreements?
   B. Structure of a Confidentiality Agreement
      1. Explanation of Purpose
      2. Disclosure
      3. No Disclosure
      4. No Use
      5. Limits on Information Deemed Confidential
      6. Term
      7. Remedies in the Event of Breach
      8. Termination