

## Practitioner's Perspective

by Holly K. Towle, J.D.



**Holly K. Towle** is a partner with Kirkpatrick & Lockhart Preston Gates Ellis LLP (K&L Gates), an international law firm, and chair of the firm's E-merging Commerce group. Holly is located in the firm's Seattle office and is the coauthor of *The Law of Electronic Commercial Transactions* (2003, A.S. Pratt & Sons). Holly.Towle@KLgates.com, 206-623-7580.

**Practitioner's Perspective** appears periodically in the monthly Report Letter of the CCH Guide to Computer Law. Various practitioners provide in-depth analyses of significant issues and trends.

## New Regulations Mandating Identity Theft Prevention Programs and Address Discrepancies and Change Requests

**Pop Quiz:** Which of the following types of companies are "creditors" or "financial institutions" under new regulations issued by the Federal Trade Commission (FTC) and each of the financial institution regulators (*e.g.*, FDIC, OCC, OTS, NCUA, FRB), such that the companies will need to develop and implement board-of-director-approved Identity Theft Prevention Programs by November 1, 2008:

- A. Automobile dealers
- B. Mortgage brokers
- C. Telecommunication companies
- D. Utility companies
- E. Banks, savings and loans, credit unions, mutual savings banks
- F. Any person holding a consumer transaction account (a deposit or account on which the accountholder may make withdrawals, make payments, or transfers to others)?

E and F are dead giveaways for "financial institutions." Most financial institutions also make loans, so E and F will typically be creditors as well. But A through D are also "creditors" under these new regulations. Why? The short answer is that the regulations so list them. The longer answer has to do with the definition of "credit" under federal Regulation B, from which this new regulation borrows. While it is not clear that the new regulation is wholly correct, anyone who allows deferred payment of a debt is a candidate for being a "creditor."

**What are the new regulations?** The new regulations concern "Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003 (FACT).<sup>1</sup> FACT amended the Fair Credit Reporting Act (FCRA), so we are really talking about FCRA. The regulations become effective January 1, 2008 but compliance may be delayed until November, 2008. The regulations were issued jointly; this column describes the FTC regulation.

**What is identity theft?** The FTC's regulations are in 16 CFR Part 681, but that part borrows the definition of "identity theft" from 16 CFR 603.2 which defines it as follows:

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

- (b) The term “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, employer or taxpayer identification number;
  - (2) Unique biometric data, such as fingerprint, voice print, 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)). (emphasis added).

**Which financial institutions and creditors must have an Identity Theft Prevention Program?** Those that offer or maintain one or more “covered accounts” must develop and implement a written program approved by their Board of Directors. For companies that don’t have boards, “Board of Directors” is defined to include a designated senior management employee.

**What is a “covered account”?** The answer, schizophrenically, covers both consumer and business accounts. The basic definition of “covered account” is this:

- (i) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and
- (ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks. (emphasis added).

The first kind of covered account looks to the creditor or financial institution’s design for the account, *i.e.*, it must be a consumer account in the traditional sense because it must be intended for use primarily for personal, family or household purposes. But the second kind of covered account is any “other account” that poses a stated risk of identity theft, and therein lies the startling part of the regulation: “other accounts” can include business-purpose accounts. This is because “account” is defined as:

- [A] continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household or business purposes. Account includes: (i) An extension of credit, such as the purchase of property or services involving a deferred payment; and (ii) A deposit account.

Words cannot express what an unusual formulation this is. The phrase “personal, family or household” purposes is part of the standard phrasing for definitions of “consumer” in typical consumer protection statutes; to slide the words “or business” in at the end of that phrase is astonishing. The “consumer” part of the phrase also eliminates the usual qualifier “primarily,” so that too is aberrant and troublesome.

Also astonishing is the context, *i.e.*, these are identity theft regulations and businesses typically do not have “personal” information or “privacy” rights. For example, what “identity” does the Google corporation have that warrants establishment of an Identity Theft Prevention Program by the utility companies providing accounts to Google? Google obviously has trade secrets, but other laws protect those; numerous fraud laws also exist to address and balance risks to both Google and the utility company against crimes by third parties.

The staff introduction indicates the regulators were thinking of small businesses and sole proprietors when they made this leap into unintended consequences. But the regulation is not expressly so qualified, and even if it were, this coverage significantly disturbs traditional consumer and privacy law balances, and should lead to more harm than benefit. For example, many small businesses and sole proprietors who are “creditors” will not (or cannot) establish compliant Identity Theft Prevention Programs for the deferred payments they extend to their often much larger customers. Consider a sole proprietor painting contractor, a small or minority-owned construction company, or a box-lunch provider to off-site corporate employees (which employees provide name and employee numbers to qualify for the lunch service), all allowing deferred or “on account” billing. Those small businesses will be “creditors” under the regulations, but will they be better off because them? They are more likely to violate them by not having a compliant Identity Theft Prevention Program than they are to benefit from exposure to “identity” theft of the business’ “identity.”

**What is an Identity Theft Prevention Program?** It must be designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account, and must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities. The ability to tailor the program to the institution or creditor is intended to signal flexibility, *i.e.*, to allow, as stated in the staff introduction to

the regulations, smaller financial institutions and creditors to tailor their programs to their operations. The elements of the program must include reasonable policies and procedures to:

- (i) Identify relevant Red Flags for the covered accounts that the financial institution or creditor offers or maintains, and incorporate those Red Flags into its Program;
- (ii) Detect Red Flags that have been incorporated into the Program of the financial institution or creditor;
- (iii) Respond appropriately to any Red Flags that are detected pursuant to [(ii) above] to prevent and mitigate identity theft; and
- (iv) Ensure the Program (including the Red Flags determined to be relevant) is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft. (emphasis added).

**What is a “red flag”?** A red flag is a pattern, practice, or specific activity that indicates the possible existence of identity theft. Given the universe of items that such a definition can encompass, “illustrative examples” (26 of them) are included in Supplement A to Appendix A of the regulation. That appendix says that the identity theft program “should” include relevant red flags from five categories. The categories are:

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

Appendix A also contains extensive guidelines that the creditor or financial institution “must consider.”

**Can everyone but financial institutions and creditors ignore these new regulations?** No. The new regulations govern two more topics, each of which covers different persons. The two other regulations are:

- Duties of users of consumer reports regarding address discrepancies.<sup>2</sup>

- Duties of card issuers regarding changes of address and replacement or additional cards.<sup>3</sup>

**What does the address discrepancy regulation concern?**

This regulation applies to “users” of “consumer reports,” *e.g.*, persons who order credit reports or background checks such as employers, landlords, financial institutions and so on (in FCRA, “consumer” includes all individuals although some aspects of FCRA are confined to individuals acting for personal and not business purposes). What is “notice of address discrepancy?” Sometimes the issuer of the report, the credit reporting agency, will provide notice of an address discrepancy. What is that? It is a defined term meaning (among other things) a notice from the credit reporting agency informing the user of a “substantial difference” between the address the user provided to request the report, and the address(es) in the credit reporting agency’s file.

For example, if an employer obtains a credit report in order to help decide whether to accept a would-be employee, and if the address for the employment applicant in the credit report received doesn’t match the address in the application, then the employer (the user) must take regulated steps reasonably to decide whether the applicant is dealing with is the same person with whom the report deals.

Users have two basic obligations with respect to “notice of address discrepancies” received. First, the user must develop and implement reasonable policies and procedures designed to enable it to form a reasonable belief that the consumer report ordered and received relates to the relevant consumer. This rule applies to new and old relationships. Second, the user must develop and implement reasonable reconciliation policies and procedures for the purpose of sending back to the credit reporting agency, a more accurate address. There are conditions to this second obligation, but even if the new regulation does not apply, other sections of FCRA might impose a similar “updating” duty. Importantly, the illustrative employer cannot simply send back to the credit reporting agency, the address that the applicant gave. Instead, the employer must reasonably try to determine what the real address is, by means specified in the regulation.

**What does the address change and replacement card regulation concern?**

This regulation applies to a financial institution or creditor that also issues a debit or credit card (*i.e.*, the coverage does not sweep in all issuers of debit cards). Although this rule involves addresses, this one speaks to address changes and requests for replacement or additional debit or credit cards. It applies in situations where the card issuer receives notice of an address change for its consumer’s debit or credit card account and, within a short time thereafter (during at least the first 30 days after receipt), the issuer receives a request for an additional or replacement card. That kind of request is perceived by Congress to be a possible indicator of

identity theft, *i.e.*, an identity thief changes the address of the real cardholder so that the real cardholder won't get her periodic statement anymore; then the identity thief orders another card and can begin to use it before the real cardholder figures out she's not getting her statements and begins to wonder why.

To deal with that and other kinds of identity theft relating to address changes, the issuer must have established and implemented reasonable policies and procedures to assess the validity of a change of address, and may not issue the additional or replacement card until it assesses the validity of the address change under those policies. It must also notify the cardholder of the request as provided in the regulation and either: (1) provide the cardholder with a reasonable means of promptly reporting incorrect address changes; or (2) otherwise assess the validity of the address change per its policies. The regulation includes some alternatives and requires any written or electronic notice to be clear and conspicuous and provided "separately" from the issuer's "regular" correspondence with the cardholder. There's a trick on the definition of "clear and conspicuous"—it's not the usual definition and is one that the financial institution regulators previously assured would be confined to use only in the Gramm Leach Bliley Act.

As with the other regulations, there is more here than meets the eye. For example, a card allowing access to a home equity line of credit can be a credit card if it meets the Regulation Z definition (which is cross-referenced by FCRA); stored value cards (such as a merchant gift card) are not yet debit cards, but the regulation takes the position that payroll cards are debit cards if the issuer also holds the consumer's account. Clear? Actual answers will result from a complex interplay between varying definitions and approaches in FCRA (as amended by FACT) and Regulation E (the regulation implementing the federal Electronic Funds Transfer Act), each of which differently defines relevant terms and each of which is undergoing regulatory or statutory expansion. In short, this is one of those areas where careful study under the particular facts and circumstances is advisable.

Also advisable is reviewing all of the new regulations. If they apply, implementation might take the time allowed.

### Endnotes

- <sup>1</sup> See 16 CFR § 681.2 and see Appendix A to Part 681—Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation.
- <sup>2</sup> See 16 CFR § 681.1.
- <sup>3</sup> See 16 CFR § 681.3.