The Fair and Accurate Credit Transactions Act: New tool to fight identity theft

Theresa J. Holt
Associate Professor and Attorney, Department of Accounting and Business Law, Cleveland State University, Cleveland, Ohio (t.holt@csuohio.edu)

Established as a federal offense by the Identity Theft Act of 1998, identity theft is a crime of fraud in which someone uses identifying information from another person to obtain credit, merchandise, and services, or even to commit criminal activities in the name of the victim. Not just an American problem, it is, says Davis (2003), a concern in the international community as well. O'Sullivan (2004) and others have raised the issue of whether the problem has been overstated. However, after the release of an FTC survey last year, little doubt remains that identity theft is widespread and is sweeping the country like an epidemic.

Released in September 2003 and based on telephone inquiries of more than 4,000 adults, the FTC survey indicates that since 1998, approximately 27.3 million people have suffered some form of identity theft. During 2002 alone, almost 10 million Americans were victims of it, with an estimated cost of $48 billion to businesses and $5 billion to consumers. How much was the loss to the average citizen or company for the same year? The FTC reports an average individual loss of about $500 and an average business loss of about $4,800.

A national fraud alert system and free annual access to credit reports are among the weapons the FACT Act provides consumers in the war on identity theft.

Of the victims in 2002, approximately 67 percent stated that their existing credit card accounts were the target, while 19 percent reported the unauthorized and illegal use of checking accounts. About 3.2 million people learned that their personal identifying information had been used to open new bank and credit card accounts. And about 2.5 million believed that identifying information had been obtained from lost or stolen credit cards, checkbooks, or social security cards.

The FTC reports that identity theft has been the number one consumer complaint for the past several years. It recorded nearly 162,000 such complaints in 2002 alone. Further reports indicate that the problem is growing every year.

Now in response to this growing problem comes the Fair and Accurate Credit Transactions Act. Also known as the FACT Act, it represents key changes in the fight against identity theft. Signed into law by President Bush on December 4, 2003, the Act amends the Fair Credit Reporting Act (FCRA) of 1970, which regulates credit report information. It also expands access to credit services and improves the accuracy of consumer credit information. Our concern here, however, is with the large part of the Act relating to identity theft. The weapons it wields are detailed below.

One-call fraud alerts

At the request of consumers or their representatives, consumer reporting agencies (CRAs)—commonly known as major credit bureaus—are now required to include fraud alerts in consumer files. A requesting consumer must assert a good faith suspicion of having been or of becoming a victim of identity theft. The fraud alert notifies all prospective report users that the consumer may be a victim of fraud, including identity theft. The statement must be pre-

sented in a manner that is both clear and conspicuous.

A duty is imposed on consumer report users to honor fraud alerts. They are not allowed to establish a new credit line or extension of credit, issue an additional card on an existing account, or increase the credit limit on an existing account unless they take reasonable steps to verify the consumer's identity.

The CRA must provide the alert along with any credit score generated in using that file. This type of fraud alert lasts up to 90 days. The consumer or representative may request removal of the alert prior to the expiration of the 90-day period. However, the agency must first receive proof of the identity of the person making the request. When the CRA places a fraud alert in the file of a consumer, the consumer is entitled to a free credit report explaining what is in the file and verifying the inclusion of the alert.

Moreover, if the consumer or representative contacts a CRA, such as Experian, the CRA must inform other CRAs that a fraud alert has been placed on the file. The consumer will no longer need to make multiple phone calls to such agencies. One call triggers notification to others—hence, the term "one-call fraud alert." However, the one-call method applies to the initial placement of the alert in the file, not to renewals.

Extended alerts

At the request of a consumer or representative, an extended fraud alert lasting up to seven years will be placed in the consumer's file, provided that an "identity theft report" is submitted to the CRA. As defined by the statute, the report alleges identity theft, is filed with the appropriate law enforcement agency, and subjects the consumer to criminal penalties if the information is false. The CRA must receive a copy of the official, valid report.

During the five-year period from the date of the request, the CRA must exclude, or "opt out," the consumer from lists provided to third parties offering credit or insurance as part of a transaction that the consumer did not initiate. The consumer does not need to take any action to activate this exclusion. However, he does have the option or choice of requesting that the exclusion be rescinded prior to the end of the statutory five-year period.

CRAs are authorized not to include the first five digits of a consumer's social security number (SSN) in their disclosures.

As with a one-call alert, the contacted CRA is required to inform other such agencies that an extended alert has been placed in the file of the consumer. However, in the case of an extended alert, the consumer is entitled to two free copies of the credit report each year.

Active duty alerts

Military consumers on active duty have special provisions. Upon request, the CRA will place an active duty alert in their files that lasts up to a year, and will be required to notify other CRAs of the alert. In addition, the consumers receive a two-year automatic opt-out from lists provided to third parties by the CRA. Like the above alert, this exclusion occurs without the need for action on the part of the consumer. The consumer also has the option or choice of requesting rescission of the exclusion prior to the end of the statutory two-year period.

Free credit report

Regardless of whether a fraud alert has been placed in his file, any consumer may request and obtain a free credit report annually. This measure provides greater access to credit information and enables consumers to review the reports for inaccuracies and inconsistencies, perhaps stopping identity thieves before they can do significant damage.

Truncation of credit and debit card account numbers

Businesses are prohibited from printing more than the last five digits of a credit card or debit card number on a receipt given to the cardholder at the point of sale or transaction. They are also prohibited from printing the expiration date on the receipt. There are some limitations to this provision, however. First, it applies to receipts that are printed electronically, not to those written by hand or that result from an imprint or copy of the card. It also contains a three-year phase-in period for older cash registers or other machines in use before January 1, 2005.

Truncation of social security numbers

CRAs are authorized not to include the first five digits of a consumer's social security number (SSN) in their disclosures. The consumer must make the request. This attempts to prevent thieves from obtaining personal identifying information from someone's mailbox.

Social security numbers are of special importance because of their identifying value. Obtaining SSNs is a common means of stealing identities. Individuals should be reluctant—should even refuse—to disclose such personal identifying information, especially this number. Such was the case in *Menton v. Experian Corporation* (2003), in which the court held that the plaintiff was required to provide proper identification to the CRA in order to obtain a credit report, but the identification did not have to be a social security number.

Red flag guidelines and regulations

Banking regulators, along with other appropriate authorities, are required to establish guidelines and regulations for financial institutions and creditors in order to identify and "red flag" possible instances of identity theft. These rules should identify patterns, practices, and specific forms of activity that indicate the possible existence of such a threat. Thereafter, in compliance with the guidelines and regulations, each financial institution and creditor is required to establish reasonable policies and procedures to identify possible risks to account holders or customers or to the safety and soundness of the business.

A card issuer is required to validate a change of address request if the request is made within a short period of time (such as 30 days) upon receiving a request for an additional or replacement card on an existing account. Validation may be made by notifying the cardholder at the former address or by using other reasonable means.

If a credit or deposit account has been inactive for more than two years, the financial institution or creditor is required to use reasonable means to notify the account holder of any sudden activity. This action is designed to reduce the likelihood of identity theft with respect to the account in question.

Preparation of consumer rights summary

The FTC, in consultation with banking agencies and others, is directed to prepare a model summary of the rights of consumers with respect to procedures relating to fraud and identity theft. Moreover, CRAs must provide consumers with this summary as well as information on how to contact the FTC.

Business record disclosure

Within 30 days of a request, a business is required to provide to both the victim and the law enforcement agency a copy of the records of any fraudulent transaction alleged to be the result of identity theft. These records are to be provided free of charge. The business is entitled to verification of the victim's identity and proof of the claim. Civil liability is not incurred by a business for disclosures made in good faith. Moreover, this provision does not impose any new recordkeeping duties on a business.

A request for records should be made in writing by the victim and mailed to the address indicated by the business. If asked by the business, the victim should include any known relevant information about the transaction in question, such as the date it occurred, the account number, and so on. In certain instances, a business may decline to provide this information, such as when it lacks confidence in the true identity of the person making the request, or believes that facts relating to the request have been misrepresented.

In an effort to coordinate identity theft complaint investigations, all CRAs must develop and maintain procedures for referring any consumer complaints to one another alleging identity theft or requesting a fraud alert or block.

Blocking

A CRA is required to block information that a consumer believes is the result of identity theft. The block (or non-reporting) must be done within four business days after receiving proof of the consumer's identity, a copy of an identity theft report, the identification of the information, and a statement by the consumer that the information does not relate to any transaction he has made. Moreover, the CRA must notify the furnisher of the information of the existence of the block. Law enforcement agencies, however, will have access to blocked information.

Under certain circumstances, a CRA may decline to block information, or may rescind a block. These circumstances include instances of error, material misrepresentation by the consumer, or consumer acquisition of goods, services, or money as a result of the block.

Coordination

In an effort to coordinate identity theft complaint investigations, all CRAs must develop and maintain procedures for referring any consumer complaints to one another alleging identity theft or requesting a fraud alert or block. The FTC, in consultation with other agencies, will develop a model form and model procedures to be used by consumers for contacting CRAs and creditors. In addition, each CRA will submit to the FTC an annual summary report on consumer complaints it has received on identity theft and fraud alerts.

Repollution

Preventing the repollution of consumer reports is a vital part of the fight against identity theft. A term commonly used in the field, *repollution* refers to reentering information about identity theft into the credit report of the victim after steps have been taken to "clean up" or purge the record of such information. Anyone furnishing information to a CRA has to set up reasonable procedures for responding to notification received from CRAs about identity

theft in order to avoid contaminating the record again. If a consumer submits an identity theft report to a furnisher, then the furnisher cannot forward the information about the theft to any CRA.

Another prohibition included in this section is that a person or business cannot sell, transfer, or place in collection a debt subject to a block resulting from identity theft. An exemption to this is the securitization of debt or the pledging of a portfolio of debt as collateral in connection with borrowing.

Debt collectors

Debt collectors are required to notify the third party for whom they work that the debt may be the result of identity theft. Upon request, they must also provide the consumer with information regarding consumer rights and the handling of disputes in debt collection.

Civil action

A legal action to enforce any of the above provisions must be brought within two years after the date the plaintiff discovers the violation or five years after the date on which the violation occurs, whichever is earlier. CRAs are encouraged to maintain records for at least six years.

The subject of identity theft raises many issues that exceed our scope here. A separate article would be needed to address them properly. Examples of important related issues that might be discussed in the future include, but are not limited to, the prevention and deterrence of identity theft, the effect of the FACT Act on e-commerce customers, public awareness of the Act's existence and application, and consumer anxieties about identity theft. ❍

References

Davis, Erin S. 2003. A world wide problem on the World Wide Web: International responses to transnational identity theft via the Internet. *Washington University Journal of Law* 12: 201-227.

Fair and Accurate Credit Transactions Act. 2003. Pub. L. 108-159, 117 Stat. 1952.

Fair Credit Reporting Act. 1970. 15 USC Sections 1681 *et seq.*

Federal Trade Commission. 2003. Identity theft survey report. @ www.ftc.gov (September).

Identity Theft and Assumption Act. 1998. Pub. L. 105-318, 112 Stat. 3007 (codified at 18 USC section 1028(a)(7).

Menton v. Experian Corporation, US Dist. LEXIS 3325 (2003).

O'Sullivan, Orla. 2004. ID theft overstated? Some think so. *ABA Banking Journal* 96/2 (February): 8.