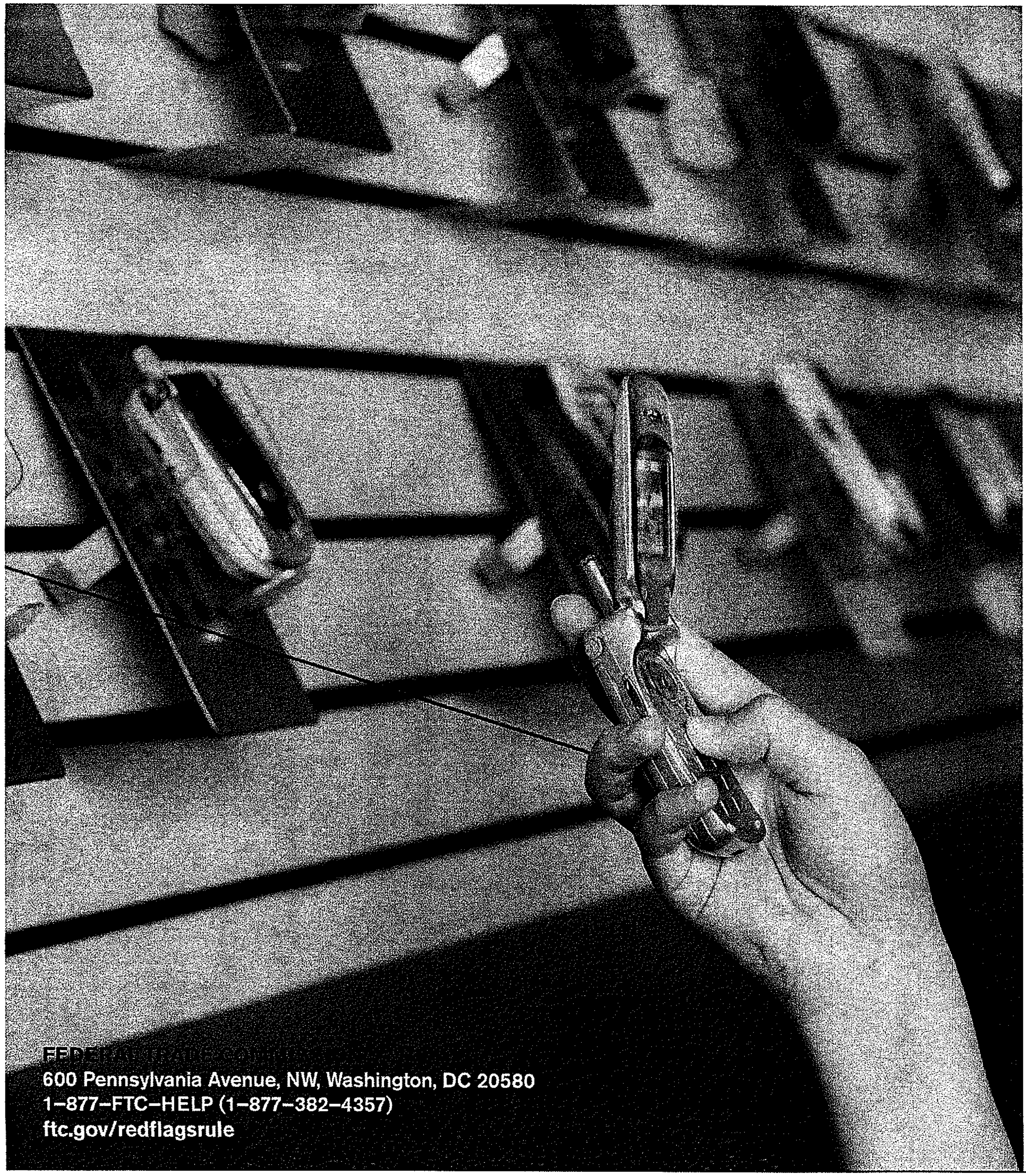

FEDERAL TRADE COMMISSION
600 Pennsylvania Avenue, NW, Washington, DC 20580
1-877-FTC-HELP (1-877-382-4357)
ftc.gov/redflagsrule

FIGHTING FRAUD WITH THE RED FLAGS RULE

A How-To Guide for Business

As many as nine million Americans have their identities stolen each year. Identity thieves may drain their accounts, damage their credit, and even endanger their medical treatment. The cost to businesses – left with unpaid bills racked up by scam artists – can be staggering, too.

The "Red Flags" Rule, in effect since January 1, 2008, requires many businesses and organizations to implement a written Identity Theft Prevention Program designed to detect the warning signs – or "red flags" – of identity theft in their day-to-day operations, take steps to prevent the crime, and mitigate the damage it inflicts.[1] By identifying red flags in advance, they will be better equipped to spot suspicious patterns when they arise and take steps to prevent a red flag from escalating into a costly episode of identity theft.

The Red Flags Rule is enforced by the Federal Trade Commission (FTC), the federal bank regulatory agencies, and the National Credit Union Administration. If you work for a bank, federally chartered credit union, or savings and loan, check with your federal regulatory agency for guidance. Otherwise, this booklet has tips for determining if you are covered by the Rule and guidance for designing your Identity Theft Prevention Program.

THE RED FLAGS RULE

An Overview

The Red Flags Rule sets out how certain businesses and organizations must develop, implement, and administer their Identity Theft Prevention Programs. Your Program must include four basic elements, which together create a framework to address the threat of identity theft.[2]

First, your Program must include reasonable policies and procedures to identify the "red flags" of identity theft you may run across in the day-to-day operation of your business. Red flags are suspicious patterns or practices, or specific activities, that indicate the possibility of identity theft.[3] For example, if a customer has to provide some form of identification to open an account with your company, an ID that looks like it might be fake would be a "red flag" for your business.

Second, your Program must be designed to detect the red flags you've identified. For example, if you've identified fake IDs as a red flag, you must have procedures in place to detect possible fake, forged, or altered identification.

Third, your Program must spell out appropriate actions you'll take when you detect red flags.

Fourth, because identity theft is an ever-changing threat, you must address how you will re-evaluate your Program periodically to reflect new risks from this crime.

Just getting something down on paper won't reduce the risk of identity theft. That's why the Red Flags Rule sets out requirements on how to incorporate your Program into the daily operations of your business. Your board of directors (or a committee of the board) has to approve your first written Program. If you don't have a board, approval is up to an appropriate senior-level employee. Your Program must state who's responsible for implementing and administering it effectively. Because your employees have a role to play in preventing and detecting identity theft, your Program also must include appropriate staff training. If you outsource or subcontract parts of your operations that would be covered by the Rule, your Program also must address how you'll monitor your contractors' compliance.

The Red Flags Rule gives you the flexibility to design a Program appropriate for your company -- its size and potential risks of identity theft. While some businesses and organizations may need a comprehensive Program that addresses a high risk of identity theft in a complex organization, others with a low risk of identity theft could have a more streamlined Program.