

provide identifying documents at the point of sale, strenuously opposed this requirement if it were interpreted to cover documents presented to the merchant. These commenters stated that copy machines are not usually available at the point of sale, and that the rule as proposed would require merchants to purchase large numbers of additional copy machines. The commenters also anticipated that consumers would be greatly inconvenienced by this requirement and might have to endure lengthy waits during any busy shopping season. These commenters questioned whether the risks of money-laundering and the financing of terrorism through retail store credit cards, which generally have relatively low credit limits, restrictions on pre-payment, and other features to detect fraud, warrant the imposition of these additional costs.

Other commenters stated that requiring banks to keep copies of documents that have pictures, such as driver's licenses, could expose the bank to allegations of unlawful discrimination, even if the retention of this information were not prohibited under ECOA. Some banks objected to this requirement on the grounds that it directly conflicted with the position that the Agencies have traditionally taken on this issue, including the criticism of banks that have retained such information in their files when extending credit.

Other commenters asked that a bank be permitted to record the processes and procedures generally used for verification rather than being required to keep records of the methods used and the resolution for each and every account, especially where the bank uses standardized procedures for all customers and could demonstrate that these procedures were applied. Some commenters suggested that the final rule permit banks to use a risk-based approach for recordkeeping.

In light of the comments received, Treasury and the Agencies have reconsidered and modified the recordkeeping requirements of the proposed rule. The final rule provides that a bank's CIP must include procedures for making and maintaining a record of all information obtained under the procedures implementing the requirement that a bank develop and implement a CIP. However, the final rule affords banks significantly more flexibility than did the recordkeeping provisions contained in the proposal. Under the final rule, a bank's records are to include "a description," rather than a copy, of any document upon which the bank relied in order to verify the identity of the customer, noting the

type of document, any identification number contained in the document, the place of issuance, and, if any, the date of issuance and expiration date. The final rule also clarifies that the record must include "a description" of the methods and results of any measures undertaken to verify the identity of the customer, and of the resolution of any "substantive" discrepancy discovered when verifying the identifying information obtained, rather than any documents generated in connection with these measures.

As Treasury and the Agencies indicated in the preamble for the proposal, nothing in the rule modifies, limits, or supersedes section 101 of the Electronic Signatures in Global and National Commerce Act, Pub. L. 106-229, 114 Stat. 464 (15 U.S.C. 7001) (E-Sign Act). Thus, a bank may use electronic records to satisfy the requirements of this final rule, as long as the records are accurate and remain accessible in accordance with 31 CFR 103.38(d).

#### *Section 103.121(b)(3)(ii) Retention of Records*

The proposal required a bank to retain all of the records specified in the recordkeeping provision for five years after the date the account is closed.

This requirement prompted strenuous objections. Assuming that copies of the documents used to verify the identity of the customer would have to be retained, commenters asserted that retaining records until five years after the account is closed would be very burdensome. Some commenters noted that imaging is not a routine practice for community banks and could be costly. Banks offering credit card accounts stated that the record retention requirement would require a change in forms, processes, and systems, while also increasing storage costs. As credit cards do not have a specific term, commenters noted that banks would be required to keep these records forever, unless they are culled manually. Some commenters suggested that the retention period be shortened, with suggestions ranging from one to three years after the account is closed, while other commenters suggested that the period be shortened to five years from when the account is opened. Many commenters stated that two years from when the information is obtained would be consistent with other regulatory requirements, such as the record retention requirements for an application for an extension of credit subject to ECOA (12 CFR 202.12(b)).

By eliminating the requirement that a bank retain copies of the documents used to verify the identity of the

customer, Treasury and the Agencies believe that the final rule largely addresses the main concern of these commenters. However, Treasury and the Agencies also have determined that, while the identifying information provided by the customer should be retained, there is little value in requiring banks to retain the remaining records for five years after an account is closed because this information is likely to have become stale. Therefore, the final rule now prescribes a bifurcated record retention schedule that is consistent with the general five-year retention requirement in 31 CFR 103.38. First, the bank must retain the information referenced in paragraph (b)(3)(i)(A) (that is, information obtained about a customer), for five years after the date the account is closed or, in the case of credit card accounts, five years after the account is closed or becomes dormant. Second, the bank need only retain the records that it must make and maintain under the remaining parts of the recordkeeping provision, paragraphs (b)(3)(i)(B), (C), and (D) (that is, information that verifies a customer's identity) for five years after the record is made.

*Section 103.121(b)(4) Comparison with Government Lists.* The proposed rule required a bank to have procedures for determining whether the customer appears on any list of known or suspected terrorists or terrorist organizations provided to the bank by any Federal government agency. In addition, the proposal stated that the procedures must ensure that the bank follows all Federal directives issued in connection with such lists.

Most commenters were concerned about how a bank would be able to determine what lists should be checked for purposes of this provision and how these lists would be made available. Some commenters asked that the final rule confirm that a bank will not have an affirmative duty to *seek out* all lists compiled by the Federal government and would only be required to check lists *provided* to it by the Federal government. Some commenters noted that lists published by OFAC are published but are not provided to financial institutions.<sup>32</sup> Many commenters urged that all lists within the meaning of section 326 of the Act,

<sup>32</sup> Nevertheless, the legislative history for this provision indicates that the lists Congress intended financial institutions to consult "are those already supplied to financial institutions by the Office of Foreign Asset Control (OFAC), and occasionally by law enforcement and regulatory authorities, as in the days immediately following the September 11, 2001, attacks on the World Trade Center and the Pentagon." H.R. Rep. No. 107-250, pt. 1, at 63 (2001).