

to delete it. For the reasons discussed below, however, the rule does require that a bank's CIP address the circumstances in which it will obtain information about such individuals in order to verify the customer's identity. Treasury and the Agencies believe that while the majority of customers may be verified adequately through the documentary or non-documentary verification methods described in paragraphs (b)(2)(ii)(A) and (B), there may be instances where this is not possible. The risk that the bank will not know the customer's true identity may be heightened for certain types of accounts, such as an account opened in the name of a corporation, partnership, or trust that is created or conducts substantial business in a jurisdiction that has been designated by the United States as a primary money laundering concern or has been designated as non-cooperative by an international body.

Obtaining sufficient information to verify a customer's identity can reduce the risk that a bank will be used as a conduit for money laundering and terrorist financing. Treasury and the Agencies believe that a bank must identify customers that pose a heightened risk of not being properly identified, and a bank's CIP must prescribe additional measures that may be used to obtain information about the identity of the individuals associated with the entity in whose name such an account is opened when standard documentary and non-documentary methods prove to be insufficient.

For these reasons, the requirement to verify the identity of signatories has been replaced by a new provision in the final rule that requires that a bank's CIP address situations where, based on the bank's risk assessment of a new account opened by a customer that is not an individual, the bank also will obtain information about individuals with authority or control over such account, including signatories, in order to verify the customer's identity. This additional verification method will only apply when the bank cannot adequately verify the customer's identity using the documentary and non-documentary verification methods described in (b)(2)(ii)(A) and (B). Moreover, a bank need not undertake any additional verification if it chooses not to open an account when it cannot verify the customer's identity using standard documentary and non-documentary verification methods.

Section 103.121(b)(2)(iii) Lack of Verification. The proposed rule stated that a bank's CIP must include procedures for responding to circumstances in which the bank cannot

form a reasonable belief that it knows the true identity of a customer. The preamble for the proposed rule listed what these procedures should include. In addition, the proposal stated that a bank should only maintain an account for a customer when it can form a reasonable belief that it knows the customer's true identity.³⁰

The final rule retains the general requirement that a bank's CIP include procedures for responding to circumstances in which the bank cannot form a reasonable belief that it knows the true identity of the customer. However, the rule text itself now states that the procedures should describe the following: when a bank should not open an account for a potential customer; the terms under which a customer may use an account while the bank attempts to verify the customer's identity; when the bank should close an account after attempts to verify a customer's identity have failed; and when the bank should file a Suspicious Activity Report in accordance with applicable law and regulation.

One commenter stated that requiring a bank to close an account if it cannot verify a customer's identity would conflict with state laws and would subject the bank to legal liability. The commenter urged that if this provision is retained, the final rule also should shield banks from state regulatory and borrower liability in these circumstances. Other commenters asked that Treasury and the Agencies clarify that further investigation that results in failure to open an account will not trigger adverse action requirements under the FCRA, 15 U.S.C. 1681 *et seq.* or the Equal Credit Opportunity Act (ECOA), 15 U.S.C. 1691 *et seq.*

The final rule does not specifically require a bank to close the account of a customer whose identity the bank cannot verify, but instead leaves this determination to the discretion of the bank. Treasury and the Agencies have determined that there is no statutory basis to create a safe harbor that would shield banks from state regulatory or borrower liability if a bank should choose to close a customer's account. Any such closure should be consistent with the bank's existing procedures for closing accounts in accordance with its risk management practices. Treasury and the Agencies also note that a bank must comply with other applicable laws and regulations, such as the adverse

action provisions under ECOA and the FCRA, when determining not to open an account because it cannot establish a reasonable belief that it knows the true identity of the customer.³¹

Section 103.121(b)(3) Recordkeeping

Section 103.121(b)(3)(i) Required Records. The proposed rule set forth recordkeeping procedures that must be included in a bank's CIP. Under the proposal, a bank would have been required to maintain a record of the identifying information provided by the customer. Where a bank relies upon a document to verify identity, the proposal would have required the bank to maintain a copy of the document that the bank relied on that clearly evidences the type of document and any identifying information it may contain. The bank also would have been required to record the methods and result of any additional measures undertaken to verify the identity of the customer. Last, the bank would have been required to record the resolution of any discrepancy in the identifying information obtained.

This section of the proposed rule prompted the most comment. Though one commenter felt that the recordkeeping requirements in the proposed rule were weak, almost all other commenters identified the proposed documentation and record retention requirements as overly burdensome. Commenters urged Treasury and the Agencies to permit a bank to record the information from the documents obtained rather than requiring banks to maintain copies of these documents for the life of the account. Commenters generally argued that it would be difficult and very burdensome to store and retrieve copies of documents used to verify the identity of the customer. In addition, some commenters noted that many kinds of identification documents, particularly some new driver's licenses, have security features that prevent them from being copied legibly. Other commenters stated that copies of documents would be difficult to safeguard and could facilitate identity theft.

Commenters stated that requiring banks to keep copies of documents would substantially deviate from current banking practice and would violate certain states' laws. Banks offering credit card accounts through retailers, who require the customer to

³⁰ The preamble also explained that there are some exceptions to this basic rule. For example, a bank may maintain an account at the direction of a law enforcement or intelligence agency, even though the bank does not know the true identity of the customer.

³¹ See 12 CFR 202.9(b) (Federal Reserve Regulation B that prescribes the form of ECOA notice and statement of specific reasons); 15 U.S.C. 1681m (FCRA provision that provides for duties of users taking adverse actions on the basis of information contained in consumer reports from other third parties or affiliates).