

CORPORATE CREDIT UNION GUIDANCE LETTER

No. 2004-02

DATE: June 2004

SUBJ: Bank Secrecy Act (BSA) Compliance

TO: The Corporate Credit Union Addressed

The purpose of this letter is to provide guidance to corporate credit unions regarding their responsibilities for Bank Secrecy Act (BSA) compliance, particularly when engaging in wire transfer activities on behalf of their natural person credit union members. The information is intended to illustrate some of the basic considerations relevant to developing an effective BSA compliance program. Each corporate credit union should consider its own business model as it evaluates and refines its existing program.

Generally, corporate credit unions are required to establish and maintain procedures reasonably designed to assure compliance with the Bank Secrecy Act and the Department of Treasury's implementing regulations. The applicable Treasury regulations may be found in Title 31, Part 103 of the Code of Federal Regulations. The basic requirements of a Bank Secrecy Act compliance program are set forth in Section 748.2(b) of NCUA's Rules and Regulations.

Establish an Effective BSA Compliance Program

Establishing an effective BSA compliance program goes beyond a written, board-approved Anti-Money Laundering Policy. Before developing a new program or analyzing the effectiveness of an existing one, it is essential to review Department of Treasury's implementing regulations in order to determine their applicability to your membership base and the services you provide. Once this is done a program can be developed that meets regulatory requirements while conforming to the specific business practices in your institution. NCUA's regulations require that all programs contain at least the following: (1) a customer identification program; (2) internal controls to assure compliance; (3) independent testing for compliance; (4) a designated individual with responsibility for monitoring day-to-day compliance; and (5) training for appropriate personnel.

Wire Transfer Services

There is some confusion about the extent of a corporate credit union's responsibility to monitor wire transfer activity processed on behalf of its member credit union members in order to identify and report suspicious activity.

Corporate credit unions provide wire transfer services to their members, natural person credit unions. Member credit unions transfer funds on behalf of their natural person members. Corporate credit unions serve as the depository financial institution (DFI) for the member credit union. The member credit union remains the DFI for the natural person member.

Typically a wire transfer is conducted through the corporate credit union, acting as the intermediary financial institution, by transferring the funds out of the credit union account with the corporate and into the Federal Reserve Bank. In that situation the originator of the transaction, the natural person credit union member, is not a member of the corporate and the corporate credit union will not have any knowledge of the normal transaction activity for that member. The responsibility for monitoring that individual member's account activity for BSA compliance and suspicious activity reporting belongs to the natural person credit union where the account is maintained.

In contrast, the corporate credit union should have knowledge of the typical account activity that occurs in the accounts it maintains for its credit union members. It has the responsibility to maintain an effective BSA compliance program that will assure appropriate monitoring, and, if necessary, reporting of suspicious transactions in connection with these accounts. As part of this due diligence the corporate credit union has a responsibility to investigate any suspicious or unusual activity it detects as part of this process. In addition, it is reasonable, in the case of non-batched transactions, to periodically review transaction records for signs of structuring among the wire transfers it has processed for its credit union members.

Effective Due Diligence and Monitoring Program

A comprehensive program of member due diligence is the corporate's most effective tool in monitoring account activity for unusual or suspicious transactions. Corporate credit unions need to employ a method for knowing the normal business activity of each member credit union. The process of identifying normal activity begins at account opening. Periodically a corporate credit union should update its member information. Without exception this information should be updated if the member makes significant operational changes. An effective monitoring program includes understanding that certain types of products and services, and certain geographic locations may be more susceptible to money laundering and/or terrorist financing activities. Greater due diligence standards should exist for members engaged in higher risk activities.

Establish Suspicious Activity Monitoring and Reporting Process

Crucial to an effective compliance program is establishing a suspicious activity monitoring and reporting process. Controls and measures must exist to identify and report suspicious transactions promptly. Corporate credit unions must

employ appropriate due diligence to effectively evaluate transactions and conclude whether to file a Suspicious Activity Report (SAR). Financial institutions are required to file SARs within prescribed timeframes. Additionally, SARs must be filed following the discovery of transactions aggregating \$5000 or more that involve potential money laundering or violations of the Bank Secrecy Act if the financial institution knows, suspects, or has reason to suspect the transaction meets the specifications outlined in 31 CFR 103.18(2). The financial institution must report suspicious activity. It need not determine if a crime has in fact occurred as that determination is the responsibility of law enforcement.

What constitutes a reasonable monitoring program will depend upon a number of factors. The size of the corporate, its business operation, the number, type, and complexity of services and transactions it provides to its members will impact what is reasonable. For example, periodic monitoring of wire detail may be acceptable for a corporate credit union with low volumes of wire activity. However, a spreadsheet or other filtering mechanism may be necessary to filter higher volumes of wire activity. Risk management should be consistent with the level of risk. Risk awareness can be best achieved by developing a risk-based anti-money laundering program.

Develop a Risk-Based Anti-Money Laundering Program

An anti-money laundering program should be structured to address the controls needed based on the risks posed by the products and services offered, members it serves, and geographical locations served. Wire transfers and international correspondent banking, private banking relationships, and electronic banking are all considered high-risk activities. The corporate should be aware of these high-risk activities when developing its program. While the corporate credit union may not be engaged in particular activities, the credit union member may have business activities classified as high-risk. Due diligence programs related to member transactions should correspond to the risk profile of member activity.

Especially high-risk businesses include Nonbank Financial Institutions, non-governmental organizations, and cash-intensive businesses. Again, the corporate credit union itself may be excluded from having high-risk businesses as members, but the member credit union may have such businesses within its field of membership. High-risk geographic locations include those identified by the Office of Foreign Assets Control (OFAC) and jurisdictions identified as non-cooperative in the fight against money laundering. Other high-risk geographic locations may be identified by management.

Evaluating the risk profile of member activity includes looking for common red flags. Following is a list of common money laundering red flags:

- Insufficient or Suspicious Information about transactions
- Efforts to Avoid Reporting or Record Keeping Requirement
- Activity Inconsistent with the Member's Business
- Changes in Financial Institution to Financial Institution Transactions
- Unusual Employee Behavior

Practical Application

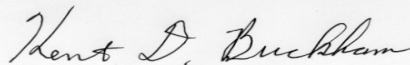
A number of readily available reports can be generated by corporate credit unions to assist them in detecting suspicious or unusual activity. As mentioned previously, a periodic review of wire records in corporate credit unions with low wire transfer activity is usually sufficient to identify unusual activity. For corporate credit unions with greater wire activity, use of spreadsheets or vendor software, is an efficient way to review wire activity for unusual patterns. Most vendor software systems include standard suspicious activity filter reports. Each corporate should establish its own filtering criteria for wire volumes based on its member base and associated risks. Non-member wire transactions and Pay Upon Proper Identification transactions should always be reviewed for unusual activity.

In addition, the initial and ongoing member due diligence should be documented. Documentation should include the normal business activities of the member and identify especially high-risk activities.

The information provided in this letter is intended for "guidance" purposes. It relates to responsibilities concerning the Bank Secrecy Act and its implementing regulations. It does not address a corporate credit union's separate responsibility to monitor transactions by and through its accounts in order to comply with OFAC regulations.

If you have any questions, please contact this office or your state regulator.

Sincerely,



Kent Buckham
Director
Office of Corporate Credit Unions

cc: State Supervisory Authorities
NASCUS
NAFCU

ACCU