



3138 10th Street North
Arlington, VA 22201-2149
703.522.4770 | 800.336.4644
f: 703.524.1082
nafcu@nafcu.org | nafcu.org

National Association of Federally-Insured Credit Unions

July 8, 2019

Policy Division
Financial Crimes Enforcement Network
P.O. Box 39
Vienna, VA 22183

**RE: Renewal without Change of the Requirement for Information Sharing
between Government Agencies and Financial Institutions
(Docket No.: FINCEN-2018-0017; OMB Control No.: 1506-0049)**

Dear Sir or Madam:

On behalf of the National Association of Federally-Insured Credit Unions (NAFCU), I am writing in response to the Financial Crimes Enforcement Network's (FinCEN) notice and request for comment on the 314(a) information sharing program. NAFCU advocates for all federally-insured not-for-profit credit unions that, in turn, serve over 117 million consumers with personal and small business financial service products. We appreciate FinCEN's commitment to safeguarding our financial system. NAFCU recognizes the importance and necessity of the 314(a) information sharing program, and wishes to comment on issues credit unions have encountered with the program. In addition, NAFCU recommends FinCEN expand the 314(b) information sharing program scope to include fraud in order to increase utility of the program.

314(a) Information Sharing Program

NAFCU members recognize that the 314(a) program has practical utility that assists local, state, federal, and foreign law enforcement with combatting money laundering and terrorist financing. FinCEN's regulations state that each law enforcement agency seeking information through the 314(a) program should include "enough specific identifiers, such as date of birth, address, and social security number that would permit a financial institution to differentiate between common or similar names."¹ Currently, credit unions are finding that law enforcement regularly provides only some of this identifying information. Often times, credit unions are only given a common name, which creates difficulties in reviewing member records. For credit unions with limited compliance resources, the task of identifying a common name can be more difficult. In addition, the chances of a false positive exponentially increase when no other identifiable information is provided besides a name. False positives are not helpful to law enforcement agencies and negate the intent of this information sharing mechanism.

¹ See 31 CFR Part 1010.520(b)(1).

Understandably, law enforcement may not have all identifiable information available when seeking information from a credit union. However, providing credit unions and other financial institutions with all the data that is required for a customer identification program (CIP) would be more helpful for all parties. The general rule for CIP is that credit unions must collect and verify enough information to form a reasonable belief that they know the identity of a member. A CIP program requires the following information to be collected and verified: name; identification number (social security number or individual taxpayer identification number); date of birth; and residential address. Although the 314(a) program generally states that law enforcement can include information such as those pieces required for CIP, the program should require the same information as CIP is available to law enforcement at the time of the request. In addition, the inclusion of a known telephone number could assist credit unions in discovering a match. The additional information would assist credit unions in differentiating between similar member names.

Lastly, law enforcement agencies have reported to NAFCU members the difficulty in placing suspects on the 314(a) list. When law enforcement agencies are unable to place a suspect on the list they must use outside channels of communication that may not be as effective. Currently, law enforcement must include documentation with the request to FinCEN showing the size or impact of the case and the seriousness of the underlying criminal activity, among other facts. In addition, law enforcement must certify that other investigative alternatives are exhausted or unavailable. Providing documentation showing the impact or seriousness of the case may be very difficult to document to FinCEN, and the reason law enforcement is seeking a 314(a) information sharing request. We encourage FinCEN to take that into account, and ensure law enforcement agencies can efficiently use this important information sharing channel.

314(b) Information Sharing Program

The voluntary 314(b) information sharing program is an invaluable tool for NAFCU's credit union members, but the utility of the 314(b) program can be enhanced by expanding the scope to allow financial institutions to share information about fraud. Sharing information regarding fraud is currently limited to situations where the fraud is part of a money laundering scheme or terrorist financing. According to NAFCU's June 2018 *Economic & CU Monitor Survey*, 89.5 percent of NAFCU members support the inclusion of fraud in the information sharing channel. Fraudulent activity has increased exponentially in recent years and credit unions are victims of fraud. Expansion is particularly helpful for those credit unions that are located in the same geographic location as the institution that suffered the harm. Fraudsters often conduct fraudulent activities at multiple institutions before an institution recognizes irregularities and raises suspicions. An expanded scope would lead to lower losses suffered and increase the chances of identifying suspects. Additionally, a more robust information sharing program would likely increase voluntary utilization by credit unions.

Credit unions continue to strengthen safeguards against fraud, but as criminal tactics evolve given technological advancements, fraudsters are able to launch increasingly creative attacks. A recent study by Pindrop found that voice fraud rates have increased by 350 percent since 2013, with the

July 8, 2019

Page 3 of 3

overall banking industry seeing a 20 percent increase.² Voice fraud has increased due to advances in artificial intelligence and machine learning. NAFCU respectfully requests FinCEN continue to ensure that the information shared in the 314(b) program remain protected. Ensuring proper protection will increase the utility of the program. As we saw in February of this year, credit union and other financial institution Bank Secrecy Act/Anti-Money Laundering officers were targets of a phishing scam. This scam appeared to mimic legitimate inquiries from other financial institutions as part of the 314(b) program. NAFCU appreciated FinCEN's review of their internal systems to make sure they were not compromised during the scam.

NAFCU appreciates the opportunity to share our members' views on this matter. Should you have any questions or require additional information, please do not hesitate to contact me at (703) 842-2249 or kschafer@nafcu.org.

Sincerely,

A handwritten signature in black ink, appearing to read 'Kaley Schafer', written in a cursive style.

Kaley Schafer
Regulatory Affairs Counsel

² See <https://www.pindrop.com/2018-voice-intelligence-report/>.