new york state society of
NYSSCPA
certified public accountants

Home of the Trusted Professional
3 park avenue, at 34th street, new york, ny 10016-5991
212.719.8300 • fax 212.719.3364
www.nysscpa.org

December 6, 2011

Financial Crimes Enforcement Network
Department of the Treasury
Regulatory Policy and Programs Division
P.O. Box 39
Vienna, VA 22183

Filed Electronically: http://www.regulations.gov

Re: Bank Secrecy Act Regulations: Definition of ''Monetary Instrument''
(31 CFR Part 1010) Docket Number FINCEN–2011–0003 RIN 1506–AB13

The New York State Society of Certified Public Accountants, representing more than 28,000 CPAs in public practice, industry, government and education, welcomes the opportunity to comment on the above captioned release.

The NYSSCPA's Anti-Money Laundering and Counter Terrorist Financing Committee deliberated the proposed rule and prepared the attached comments. If you would like additional discussion with us, please contact Sean M. O'Malley, Chair of the Anti-Money Laundering and Counter Terrorist Financing Committee, at (212) 720-2000, or Ernest J. Markezin, NYSSCPA staff, at (212) 719-8303.

Sincerely,

NYSSCPA
Richard E. Piluso
President

Attachment

new york state society of
NYSSCPA
certified public accountants

Home of the Trusted Professional
3 park avenue, at 34th street, new york, ny 10016-5991
212.719.8300 • fax 212.719.3364
www.nysscpa.org

COMMENTS ON

BANK SECRECY ACT REGULATIONS:
DEFINITION OF ''MONETARY INSTRUMENT''

(31 CFR PART 1010)

DOCKET NUMBER FINCEN–2011–0003 RIN 1506–AB13

December 6, 2011

Principal Drafters

Alan W. Greenfield
Linda Silvestri
J. Raymond Krozak (*Advisor*)
Sean M. O'Malley (*Advisor*)
Michael Shiely (*Advisor*)
Shonda Wade (*Advisor*)

NYSSCPA 2011 – 2012 Board of Directors

Richard E. Piluso, *President*
Gail M. Kinsella, *President-elect*
Scott M. Adair, *Secretary/Treasurer*
Anthony Cassella *Vice President*
Neville Grusd, *Vice President*
J. Michael Kirkland, *Vice President*
Ita M. Rahilly, *Vice President*
Joanne S. Barry, *ex officio*
Ian J. Benjamin
Shari E. Berk
Robert W. Berliner
Sherry L. DelleBovi
Domenick J. Esposito
Adrian P. Fitzsimons
Stephen E. Franciosa
Jennifer R. George
Rosemarie A. Giovinazzo-Barnickel
Mitchell L. Gusler
Timothy Hedley
Douglas L. Hoffman
Eric M. Kramer
Mark G. Leeds
Elliot A. Lesser
Michele M. Levine
Pei-Cen Lin
Heather Losi
Anthony J. Maltese
Barbara A. Marino
Steven M. Morse
Robert R. Ritz
Michael F. Rosenblatt
Erin Scanlon
Cynthia Scarinci
John S. Shillingsford
Robert E. Sohr
George I. Victor
Jesse J. Wheeler
Margaret A. Wood
F. Michael Zovistoski

NYSSCPA 2011 – 2012 Consulting Services Oversight Committee

Yigal Rechtman, *Chair*
Edward G. Donnelly
Martin Leventhal
Sean M. O'Malley
Lee G. Zimet

NYSSCPA 20111 – 2012 Anti-Money Laundering and Counter Terrorist Financing Committee

Sean M. O'Malley, *Chair*
Michael J. Angerhauser
Joseph P. Athy
Christopher M. Bailey
S. David Belsky
Jack M. Carr
Kevin P. Caulfield
Steven B. Chatwin
William L. Del Gais
Marc A. Engel
Howard M. Gluckman
Robert L. Goecks
Alvin H. Goldman
Peter A. Goldman
Wendy Grant Mungroo
Alan W. Greenfield
Audrey Greif
Susan Havranek
Peter F. Heuzey
Richard E. Hurley
Norman V. Jardine
Patricia A. Johnson
Richard Kando
Dennis B. Kremer
Cynthia L. Krom
J. Raymond Krozak(*Advisor)*
Nancy Leo
Carrie Malachowski
David Mendelsohn
Philip J. Musacchio
John M. Perrone
Joseph R. Petrucelli
Rona Pocker
Barry L. Pulchin
Bobbie L. Sheils
Michael Shiely *(Advisor)*
Linda Silvestri
Jeffrey Sklar
Sheryl Skolnik
Carol Tanjutco
Ann Marie Tricarico
Lydia M. Washington
Eva Weiss
Jeff Werner (*Advisor)*
Robin L. Zone

NYSSCPA Staff

Ernest J. Markezin

New York State Society of Certified Public Accountants

Anti-Money Laundering and Counter Terrorist Financing Committee

Bank Secrecy Act Regulations: Definition of ''Monetary Instrument'' (31 CFR Part 1010)

The Financial Crimes Enforcement Network ("FinCEN") is proposing to amend the definition of ''monetary instrument'' in the Bank Secrecy Act (''BSA'') regulations for purposes of the international transport of currency and monetary instrument reporting requirement to include tangible prepaid access devices. We are pleased to provide the following responses to questions A. through H. of Part IV, Questions for Public Comment, of the proposed rulemaking.

A. We are in agreement that at present a branded open loop prepaid access card may be indistinguishable from a traditional credit or debit card. To assist border agents and other law enforcement authorities in identifying the prepaid access instruments from traditional credit or debit card it would be necessary to work with banks and other card issuing entities to change the appearance of the prepaid instruments. This could be achieved by requiring that prepaid access instruments have different prefixes or suffixes in the card number that will differentiate the card or device from the traditional debit or credit card. This would allow these instruments to be easily identified as prepaid access instruments saving border agents and other law enforcement agencies the time it would take to scan all cards to identify which ones fall under the rule as proposed cash equivalents. This may also alleviate problems that may arise with bank cards issued in countries where financial institution privacy laws prohibit the access of certain financial information. If such a problem does arise regarding the accessing of financial information, especially available account balances on a prepaid access instrument from certain countries, FinCEN should consider putting restrictions on the use of those prepaid access cards in the United States.

   The requirement of providing the proper technology at the border(s) to access balances for the cards and for other novel devices will present an initial cost to the government and could be slightly burdensome, albeit necessary for this rule to be effective. We note that it is the obligation of the traveler to make a declaration when carrying more than the maximum allowable amount. To minimize the chance that a traveler could inadvertently carry a card with more than $10,000 across the border, we suggest that the U.S. government offer public access to such terminals at international airports and border crossing to provide the traveler with the means of determining the value on cards they are carrying[1]. The initial cost of the equipment required to read the balance on the cards and other related instruments could be paid for by the forfeiture of the additional pre-paid access cards.

[1] This would provide the traveler with the ability to determine if a third party, such as an employer or parent added value to his or her card without their knowledge.

Border officials would not have the personnel to check every traveler, so they would only need to determine the value of the card for spot checks or when there are other red flags associated with the traveler.

Another possible option that FinCEN could consider is requiring all issuers of prepaid access cards in the United States have maximum limits associated with these cards and products, not to exceed $10,000. If a bank or MasterCard or Visa has a process that specifically limits a maximum value of X (use $7,500 for this example) for a prepaid access card, then it can be absolutely known to the carrier, and to the enforcement personnel, that the value of a single prepaid access card cannot exceed the current reporting limit of $10,000. Obviously, if an individual is carrying multiple cards, this limit could be thwarted. It would be preferable to require an easily identifiable list of card numbers (possibly using Issuer Identification Numbers ("IIN") for U.S. financial institutions[2]) which would allow law enforcement to know which cards would be subject to these maximum thresholds. As discussed above, if open looped prepaid value cards (such as payroll cards), have a maximum value on them (preferably preprinted on the face of the card) that falls below the legal threshold for declaration, then a single card will represent a lower risk. However, the rules should state clearly that these cards must be included and declared, if the aggregate value of currency and prepaid access card(s) exceed the reporting thresholds.

B. A closed loop card should be considered the same as any other restricted use asset. While it is true that these cards can be sold (most likely at a discount) for cash, this can also be said of any other asset. At this time, we do not believe that closed loop cards should be considered a proposed cash equivalent.

C. Even though a branded open loop reloadable card, embossed with the name of the person to whom it was issued, does provide a moderate audit trail and accountability of the funds available to that individual, we have seen in many other money laundering schemes where organizations do utilize the equivalent of "mules" to facilitate many of their asset transfer schemes. By utilizing mules for the transfer of these types of cards, large amounts of proposed cash equivalents could easily be moved across the borders of the United States as these cards do and can function as bearer instruments in day to day commerce. Therefore, these branded open loop reloadable cards / products should be viewed as cash equivalents.

   We believe that the only reason FinCEN could decide to exclude branded open loop reloadable cards embossed with the name of the owner is if it requires the issuer to conduct due diligence on that cardholder which is equivalent to an individual who possesses a debit card attached to a bank account. If branded open loop reloadable cards require the same "know your customer" information as a debit card attached to a bank account, then it would be hard to distinguish the difference between a branded reloadable card embossed with the name of the owner and that of an individual with a bank account

[2] The first 6 digits of a credit card number are known as the Issuer Identification Number (IIN), previously known as bank identification number (BIN). These numbers identify the institution that issued the card to the card holder.

and debit card. It would be just as easy for an individual to move funds internationally with the debit card as with the branded reloadable card embossed with the owner's name. The requirement of adding branded reloadable cards embossed with the owner's name with proper due diligence requirements to the Report of International Transportation of Currency and Monetary Instruments (CMIR) requirement could create a burden on international travelers and duplicate an already existing audit trail.

D. Many prepaid access programs, whether open or closed loop, allow value to be added remotely to the funds accessible via the card or other proposed cash equivalent instrument. While the majority of the cards used in this scenario are probably legitimate and not involved with money laundering, similar to the scenario described in C., these cards can easily be used by criminal organizations to transfer funds using the mule equivalents. However, as discussed above, to allow travelers to determine if a trusted third party, such as a parent, added funds to their prepaid access card, the government should offer the traveling public access to terminals which would show the value on the card. This would provide for increased compliance and minimize the burden on travelers and border agents.

   FinCEN may also want to consider changing the Customs Declaration to specifically ask all travelers if they are carrying prepaid access cards or devices. A follow up question could ask if the maximum allowable (loadable) value of these instruments exceeds the CMIR thresholds. Another question could then ask if the aggregate value of these prepaid access cards or devices plus currency carried exceed the reportable CMIR threshold values. Perhaps, requiring the maximum value to be embossed on the card (or other proposed cash equivalent instrument) would assist the traveler in completing this filing.

   Currently, there are two different methods to value a pre-paid card: (1) funds currently available on the card and (2) the maximum amount that can be loaded on to the card. This may create confusion for travelers at border crossings. With that in mind, the border declaration obligation should be clearly set at the funds currently available on the cards. As noted in the question for comment, certain cards can be loaded online, and this transaction alone would leave an audit trail. However, given the international presence of most financial institutions it is also possible that an individual could purchase the card abroad and the money could then be loaded remotely onto the card. Providing travelers with access to a terminal at the border crossing would avoid unintentional violations of border declarations. International records of these transactions might be available, but would be difficult for law enforcement to obtain. Clearly, the greatest concern for law enforcement is individuals purchasing the prepaid cards with large amounts of cash and then taking the cards through a border crossing where it is then turned back into cash once the international border has been crossed. This proposed regulation would help achieve that goal if the Custom Declaration limits regarding open looped prepaid access devices are clear to travelers, and the U.S. government can provide travelers with a quick and efficient way to determine the current value of cards/devices in their possession.

E. As there may soon be the potential for a code or password, or object not typically associated with payment system access (*e.g.*, cell phone or key fob), to be brought into or taken out of the United States and used to access cash drawn from a prepaid access program either via an ATM or otherwise. We believe that border declaration regulations should cover all open looped prepaid devices not requiring extensive due diligence by U.S. financial institutions and this has been covered in prior sections.

F. No comment.

G. As these proposed cash equivalent instruments strongly mimic traveler's checks, the same rules and regulations regarding the shipment of traveler's checks are a logical conclusion.

H. The requirement of a PIN should not have any impact on the FinCEN regulations. It does not alter the cash equivalent of the device. For those using these devices as part of a money laundering scheme, the transmittal of the PINs is not a difficult task.