September 2011

Countering Terrorist Financing: Progress and Priorities

Questions for the Record

From Senator Charles Grassley

To Assistant Secretary Daniel L. Glaser, United States Department of Treasury:

<u>(1) Prepaid Access Card Regulations</u>

Prepaid access cards have proliferated since the 1990's and can often attract people such as college teens and individuals who prefer to avoid the banking system. These cards can be accessed without the traditional need of a bank account and can be used at point of sale terminals to purchase goods and services. Additionally, many prepaid access cards, specifically cards that are "open-loop" which means money is stored in a pooled account and not directly on the card, are used by criminals to commit money laundering. Criminals can use prepaid access cards to easily integrate illegal proceeds into the financial system so that they eventually appear legitimate. The Financial Crimes Enforcement Network recently established prepaid access card rules that were mandated by the Credit Card Accountability Responsibility and Disclosure Act of 2009. The new rules are tentatively effective on September 27, 2011.

1. The new regulations for prepaid access cards require providers to register as a Money Service Business. Why did the Financial Crimes Enforcement Network (FinCEN) exclude sellers of prepaid access cards from registering as a Money Service Business (MSB)?

   In the Prepaid Access Rule, FinCEN distinguishes between the prepaid access program provider and the seller of prepaid access in the same way other money services business (MSB) regulations distinguish between principals and agents, whereby the principal is the entity with the registration requirement. With respect to prepaid access, the program provider is analogous to the principal and the seller to the agent. As with other MSB principals, providers of prepaid access will be required to maintain lists of agents, and provide that information upon request to FinCEN, its delegate or an appropriate law enforcement agency.

2. The modified definition of prepaid access cards essentially designates the cards as a "device or vehicle to access prepaid funds". Does that now make them subject to the regulations governing financial instruments and thus subject to International Transportation of Currency and Monetary Instrument Reports (CMIR)?

For clarity FinCEN chose first to introduce the new terminology and regulatory obligations associated with prepaid access program providers and sellers of prepaid access, and will separately propose amending the definition of "monetary instrument" for purposes of the international transport of currency and monetary instrument reporting ("CMIR") requirement at 31 CFR 1010.340 to include tangible prepaid access devices. That Notice of Proposed Rulemaking was issued on October 12, 2011 and is open for a 60 day comment period.

3. Criminals frequently purchase "closed loop" prepaid access cards with stolen credit cards, and then use them to purchase items for sale, which integrates unlawfully obtained proceeds into legitimate businesses. Do you agree that "closed loop" prepaid access cards are a risk for money laundering schemes, thereby evading financial transparency?

   Many of the comments received to the Notice of Proposed Rulemaking indicated closed loop prepaid access offers very limited criminal or money laundering opportunities. Commenters noted that closed loop prepaid access typically involved relatively low dollar amounts, most commonly issued in denominations of $500 or less. Such low dollar limits and the inability except under de minimis situations required by state laws to convert closed loop prepaid access to cash make it an inefficient, cumbersome tool for use by money launderers. However, FinCEN understands that, so long as closed-loop prepaid access can be issued in denominations large enough to be of concern for schemes such as those outlined in this question, the entire category cannot be excluded from regulation. Accordingly, FinCEN has chosen to set a dollar threshold of $2,000, so that closed loop prepaid access that is issued in amounts of $2,000 or less will be excluded from the definition of prepaid program, while larger denomination programs are covered. This helps address the concerns of both retailers and law enforcement. In addition, the sale of closed loop and open loop products both figure into a separate $10,000 threshold per person per day that can trigger regulatory requirements for sellers.

<u>(2) The Use of Suspicious Activity Reports (SARs) to Detect Terrorist Financiers</u>

In the written testimony of FBI Acting Assistant Director Boelter, he states that "Suspicious Activity Reports have been important components in our efforts to identify terrorist financing." He also states that Suspicious Activity Reports are "critical tripwires to detect possible terrorist financiers as well as identifying associates of known terrorists."

1. Do you agree with Agent Boelter's statement about the value of Suspicious Activity Reports to assist in identifying terrorist financiers and associates?

Yes. Suspicious activity reports, as well as other reporting required under the Bank Secrecy Act, are consistently cited by law enforcement as integral to their efforts in investigating financial crime including the financing of terrorism.

2. Does the Department of Treasury use Suspicious Activity Reports for this purpose?

   With the exception of the Criminal Investigative Division of the Internal Revenue Service (IRS-CI), the Department's Office of the Inspector General (OIG), the Treasury Inspector General for Tax Administration (TIGTA), and the Special Inspector General for the Troubled Assets Relief Program (SIG-TARP), the Department of the Treasury does not have law enforcement personnel who conduct criminal investigations. IRS-CI makes extensive use of suspicious activity reports and other BSA data in its criminal investigations. Additionally, several components of the Office of Terrorism and Financial Intelligence (TFI) utilize suspicious activity reports and other BSA data in furtherance of their missions: the Office of Intelligence and Analysis (OIA) makes use of the data in its analytical efforts relating to terrorism and organized crime; the Office of Foreign Assets Control (OFAC) uses the data in support of its efforts to enforce economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States; and the Financial Crimes Enforcement Network (FinCEN), conducts its own analysis and also provides analytical support to law enforcement.

3. Does the Treasury have a database that collects Suspicious Activity Reports information?

   The BSA, enacted in 1970, authorizes the Secretary of the Treasury to require certain records or reports, including SARs, where they have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, or in the conduct of intelligence or counterintelligence activities, including analysis, to protect against international terrorism. FinCEN maintains the database that houses those reports and administers access to that data.

4. How does the Treasury generate new investigative leads from the vast volume of Suspicious Activity Reports?

   As noted above, with the exception of IRS-CI, OIG, TIGTA and SIG-TARP, the Department of the Treasury does not have law enforcement personnel who conduct

criminal investigations. Federal law enforcement agencies generally have direct access to SARs and other BSA data maintained by FinCEN. Law enforcement agencies inspect SARs and other BSA data for investigative leads either individually or together in SAR review teams – and many of the latter have significant IRS-CI participation. FinCEN proactively queries BSA data and provides analytical support to law enforcement investigations.

5. How does the Treasury mine the Suspicious Activity Reports data so that it is useful?

   As noted above, FinCEN has analysts who both proactively query SAR and other BSA data, as well as provide direct analytical support to federal, state, and local law enforcement investigations. Other offices within TFI (OIA, OFAC, and TFFC) also utilize SAR and other BSA data in support of their respective missions.

6. Does the Treasury participate on any task forces, committees, or working groups that use Suspicious Activity Reports to target terrorism or terrorism financing? If so, please describe those activities and relationships.

   Treasury participates in a number of law enforcement task forces that could be relevant to counter-terrorism investigations. These include the Criminal Investigations Division of the Internal Revenue Service (IRS-CI), which is involved with:

   (i) ***<u>Joint Terrorism Task Forces (JTTFs),</u> which are FBI-led cells of locally based investigators and support personnel from dozens of U.S. law enforcement and intelligence agencies. IRS-CI has 18 liaisons and 44 full-time or part-time agents assigned to the JTTFs The IRS-CI Lead Development Center in Garden City, NJ supports the IRS-CI JTTF liaisons with financial research and analysis drawing heavily on SARs and other BSA data, as well as tax information.***

   (ii) ***<u>Organized Crime Drug Enforcement Task Forces (OCDETF)</u>, which target high priority money laundering or narcotics trafficking organizations. The OCDETF Fusion Center gathers, stores, and analyzes all-source financial investigative information and intelligence, including SARs and other BSA data to support coordinated, multi-jurisdictional investigations.***

   (iii) ***<u>The Special Operations Division (SOD)</u>, a Drug Enforcement Administration-led coordination center that manages and develops programs directed against***

major national or international drug trafficking organizations. SOD uses SARs and other BSA data to support financial investigations.

FinCEN also has six analysts assigned to designated High Intensity Financial Crimes Areas (HIFCAs) in New York, Chicago, Puerto Rico, San Francisco, Los Angeles, and the Southwest Border. These analysts participate in SAR Activity Review Teams, which review new SAR filings for their respective geographical area. FinCEN personnel also participate in the Northern VA SAR Review Team, the Northern District of West Virginia SAR Review Team, and Northern District of West Virginia Working Group. All of these entities review SARs to identify potential criminal activity and while they are not solely focused on terrorism or terrorism financing, they would investigate or refer those matters, if identified.