Client Alert.

July 12, 2013

Inter-Governmental Task Force Recommends Extending Anti-Money Laundering Measures to Telecoms, Software Companies and Other Non-Traditional Mobile Payments Providers

By Rick Fischer, Obrea O. Poindexter, Barbara R. Mendelson and M. Sean Ruff

The Financial Action Task Force ("FATF") recently released a white paper entitled "Guidance for a Risk Based-Approach: Prepaid Cards, Mobile Payments and Internet-based Payment Services" ("Guidance").[1] The Guidance contains non-binding suggestions for policy makers on ways to improve their respective country's money laundering controls by applying existing FATF Recommendations to new and emerging financial services providers.[2] Because the FATF is an inter-governmental body and the United States is an active member, the Guidance has important implications for non-banks and service providers that are expanding into the mobile payments space, especially those who are offering products that do not neatly fit within the existing Bank Secrecy Act ("BSA") and anti-money laundering ("AML") requirements set forth by the Financial Crimes Enforcement Network ("FinCEN") and other federal offices such as the Office of Foreign Assets Control ("OFAC").

OVERVIEW OF THE GUIDANCE

The Guidance is meant to explain how the risk-based AML principles in the existing FATF Recommendations can be applied to each of these three payment types. The document consists of seven sections, which can be summarized as follows:

- The first three sections of the Guidance are largely table setting and provide background on the types of entities that are involved in each type of payment. For example, for mobile payments, the Guidance explains that mobile network operators, distribution channel participants (*e.g.*, retailers and software companies), and electronic money issuers (*e.g.*, banks, program managers and money transmitters) are all involved in various parts of the mobile payments transaction chain. The Guidance also identifies participants in the transaction chains for prepaid card and Internet-based payment services.

- The fourth section discusses features of each payment type that, in FATF's view, can give rise to heightened money laundering and terrorist financing risks, including anonymity, cash access (*e.g.*, via ATM transactions) and cross-border functionality. This section of the Guidance includes a "risk matrix" that FATF produced in 2010 as part of an earlier report on emerging payment methods. The matrix aligns different criteria with higher and lower risk factors. For example, for the "value limits" criteria, the matrix indicates that limitations on transaction velocity and the amount of funds that can be held in an account can reduce money laundering and terrorist financing risks. Importantly for

[1] *See* http://www.fatf-gafi.org/documents/documents/rba-npps-2013.html.
[2] For the existing FATF recommendations, *see* http://www.fatfgafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf.

mobile payments, the risk matrix highlights activities and services such as peer-to-peer transmissions, acceptance of anonymous funding sources and a high number of accepting merchants as high-risk factors in need of adequate AML controls. The suggested controls mentioned in the Guidance include an increased use of customer due diligence, load, value and geographical limits and restrictions on the types of funding sources mobile payments participants should accept.

- In the fifth section of the Guidance, FATF urges countries to consider the impact of AML requirements, and advocates for a risk-based regulatory approach that would not inadvertently, or unnecessarily, adversely impact the operations of existing products, limit the development of new products, or diminish financial inclusion. In this regard, FATF's views could provide helpful support for those industry participants who wish to express concerns in comment letters on overly restrictive regulatory requirements for mobile payments from FinCEN and other regulators.

- The sixth section provides FATF's views on the application of the existing FATF Recommendations to each of the payment types addressed in the Guidance. For example, Recommendation 16, which addresses wire transfers, recommends that financial institutions prohibit transactions with designated persons and entities. FATF explains that mobile payment and Internet-based payment service providers that are money value or transfer service providers should be subject to Recommendation 16. However, according to FATF, Recommendation 16 is not intended to cover transfers from a prepaid card for the purchase of goods and services. Similarly, the Guidance discusses applying Recommendation 10 (customer due diligence measures) to additional participants in the mobile payments chain, such as mobile network operators, as "providers of mobile payment services, whether prepaid or post-paid, typically establish business relationships with customers as envisaged by Recommendation 10."

- The seventh section provides FATF's views on how countries could implement a risk-based approach to AML for the payment types discussed in the Guidance. The Guidance states that there is a greater need to apply normal regulatory requirements (*e.g.*, perform know your customer checks and due diligence) the closer the functionality of a payment type has to a traditional bank account. The Guidance lists the following factors as demonstrating functionality similar to a bank account:

    - The payment product can be reloaded an unlimited number of times;
    - No or very high funding, loading or spending limits are applied to the product;
    - It is possible to make and receive funds transfers cross-border, and within the country where the product is issued;
    - The product can be funded through cash, and cash can be withdrawn through an ATM network; or
    - The user has the ability to add or withdraw funds from the account using cash or cash equivalents, whether directly or through another provider or intermediary.

- The recommendations for mobile payments in the seventh section are based on what types of services an entity is providing. For example, the Guidance recommends that countries subject those entities providing person-to-person transfers to licensing and full AML measures. Similarly, FATF recommends that mobile network operators be subject to AML measures, including licensure, for mobile payments conducted through telecom services (*e.g.*, carrier billing that allows person-to-person or person-to-bank transfers). FATF recommends this because it views the mobile

network operator as the entity providing the service, managing the customer relationship, holding customer funds and resolving customer claims. The Guidance also contains implications for retailers and software companies that serve as customer touch points, as it also recommends that the mobile payments entity which has visibility and management of the payment service, and which maintains relationships with customers, should be subject to AML requirements.

Contact:

Rick Fischer
(202) 887-1566
lfischer@mofo.com

Obrea O. Poindexter
(202) 887-8741
opoindexter@mofo.com

Barbara R. Mendelson
(212) 468-8118
bmendelson@mofo.com

M. Sean Ruff
(202) 778-1665
sruff@mofo.com

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials in many areas. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer*'s A-List for 10 straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.