THE IMPACT OF NEW PAYMENT PRODUCTS AND SERVICES ON MONEY LAUNDERING PREVENTION MEASURES IN MEXICO

by

Steven Eisenhauer

A Capstone Project Submitted to the Faculty of

Utica College

December 2016

in Partial Fulfillment of the Requirements for the Degree of

Master of Science in Financial Crime and Compliance Management

Abstract

While providing new methods for conducting transactions beyond traditional services offered by banks, new payment products and services (NPPS) such as prepaid cards, mobile payments and Internet-based payments, also represent challenges to many nations' existing anti-money laundering (AML) regimes. As NPPS further penetrate the economy and erode the domination of traditional financial institutions, Mexico, like all other countries, will need to evaluate the effectiveness of currently existing money laundering control measures to address the risks of these products and services. This research project sought to answer three principal questions. What are the money laundering risks presented by NPPS? What strategies and measures can be implemented by a country to combat the money laundering risks posed by NPPS? Are the various NPPS contemplated and covered by Mexico's AML regulatory framework? An extensive review and analysis of relevant literature was conducted, including academic literature, industry participant reports, international organization guidance and related laws, regulations and directives. The research project concluded that Mexico is largely prepared to address the money laundering risks of NPPS and its current money laundering control measures partially or fully address all recommended risk mitigating controls. The research project provided recommendations to ensure that all recommended mitigating controls are fully addressed as well as areas in which future research is required.

Keywords: Financial Crime and Compliance Management, Paul Pantani, emerging payment technologies (EPT), Financial Action Task Force (FATF), customer due diligence (CDD), financial inclusion.

Table of Contents

The Impact of New Payment Products and Services on Money Laundering Prevention Measures in Mexico

The introduction of new payment products and services (NPPS) threatens the anti-money laundering (AML) efforts of many countries (Financial Action Task Force, 2013). NPPS, also known as new payment methods (NPM), new payment technologies (NPT) or emerging payment technologies (EPT), refers to products and services that may be offered by, or in conjunction with, non-bank and non-traditional financial institutions, such as prepaid stored value, mobile payment systems and other Internet-based payment services. While many of these products and services are not cutting-edge nor truly new, they are considered to be NPPS because they are offered by entities other than banks (Financial Action Task Force, 2010). Kim-Kwang Raymond Choo (2013), an Associate Professor at the University of South Australia and holder of the Cloud Technology Endowed Professorship at the University of Texas at San Antonio, asserts that as global governments improve legislation and regulatory oversight of traditional banking organizations and products, criminal organizations will seek to utilize providers of NPPS to launder illicit funds, especially in jurisdictions where these products and services are less regulated. It can therefore be reasoned that any country which neglects to regulate providers of NPPS is potentially creating a legislative loop-hole that would encourage criminal actors to move their funds away from traditional financial service providers to circumvent money laundering control measures (Choo, 2013).

Like other countries, Mexico will be faced with the need to address the risk of money laundering posed by NPPS. Cash payments continue to dominate the Mexican economy, with estimates of up to 70% of transactions in certain sectors conducted in cash (Del Angel, 2016). The prevalence of the use of cash in the Mexican economy suggests a concentration of money

laundering risks related to cash deposits and a need to focus money laundering measures on traditional banking and remittance product and service providers. On the other hand, it is naïve and dangerous to assume that criminal organizations will limit themselves to the same financial products and providers utilized by most legitimate economic participants, especially in the face of increasing measures to control these means (Choo, 2013). Further, evidence suggests that although it is a nascent industry, NPPS is growing in Mexico. Over two million Oxxo branded prepaid cards, offered by the popular convenience store, have been sold in just two years. Other recent NPPS offerings in the country include an Internet-based payment service similar to PayPal, known as MercadoPago, and the innovative use of convenience stores, like Oxxo, to act as payment processors for online transactions to be settled in cash at storefronts (Harrup, 2016). Additionally, a service known as Sr. Pago allows small merchants to process credit card payments over the Nextel network and receive cash payouts at Oxxo stores without needing to open a bank account (Laya, 2015).

Beyond the moderate growth in the use of NPPS in the country, the potential for further growth is outstanding. The two main factors that sustain this potential include Mexico's poor level of financial inclusion and high rate of technology enabler penetration. It is estimated that 86% of the population in Mexico are mobile phone subscribers compared to only 18.7% which report having a bank account at a formal financial institution (Suárez, 2016). Others estimate the rate of adults with bank accounts to be closer to 39%, which remains far less than other countries in the region and significantly below the mobile subscriber rate (Wladawsky-Berger, 2016). This difference represents a large potential market for mobile payment services and provides an example of the growth potential for other NPPS to serve the underbanked population of Mexico (Suárez, 2016).

The purpose of this research project was to scrutinize AML measures implemented in Mexico in order to assess the preparedness of the country to respond to the threat of abuse of new payment products and services. This project attempted to answer these questions: What are the money laundering risks presented by new payment products and services? What strategies and measures can be implemented by a country to combat the money laundering risks posed by new payment products and services? Are new payment products and services contemplated and covered by Mexico's AML regulatory framework?

The literature available for conducting this research included international organization reports and guidance, Financial Action Task Force (FATF) country mutual evaluation reports, assessments of the risks posed by NPPS performed by industry participants, international and non-governmental organizations, scholarly articles regarding money laundering in Mexico, scholarly articles regarding NPPS, scholarly articles regarding the money laundering risks of NPPS, Cameron Holmes' book analyzing the economic threat posed by organized criminal organizations in Mexico, and primary sources including the relevant Mexican legislation, implementing regulations, and administrative rulings.

Evaluating the preparedness of Mexico to respond to the money laundering risks of NPPS can benefit multiple audiences. The Mexican financial regulatory institutions, legislators and law enforcement can benefit from this research. Additionally, compliance professionals and foreign diplomats with an interest in reducing the incidence of organized criminal activity in Mexico will find this research useful. Finally, legislators and financial sector regulatory institutions in other countries, as well as researchers considering similar topics may be able to apply the framework developed in this paper to evaluate the preparedness of other nations and regulatory regimes.

New Payment Products and Services

The FATF (2010) generally describes NPPS as prepaid cards, mobile payments and Internet-based payment services, with each category either narrowed or broadened by explanations of coverage by the organization's guidance. This project adopts the FATF definition of NPPS, including a focus on payment products and services within those three categories that are offered, at least in part, by non-financial institutions. At the same time, technological approaches to accessing traditional banking products and services, such as transacting with a checking or savings account via an Internet interface or mobile application, also known as online or mobile banking, are not considered NPPS (Financial Action Task Force, 2010).

Prepaid cards. Prepaid cards operate in either a closed-loop or open-loop model. Closed-loop prepaid cards are limited to use at specific retailers or groups and are not linked to any payment network, such as Visa or MasterCard. Open-loop cards are often linked to a payment network and therefore may be negotiable internationally. Both open- and closed-loop cards can be reloadable or single use, depending on the product. Prepaid cards have a wide range of uses from in-store gift cards to money transmission and payroll disbursement (The Wolfsberg Group, 2011).

Prepaid cards pose money laundering risks related to the relative or complete anonymity afforded to the customer and the anonymity of cash funding for prepaid accounts, the potential international use of the product, the ability to withdraw funds in cash, and the cross-border transportability of the access media. The segmentation of services inherent to the product when multiple parties are involved including acquirers, distributors, payment networks, issuers, program managers and sometimes agents, poses further risk as it is not always clearly defined

which party, if any, is responsible for complying with AML regulations and directives (Financial Action Task Force, 2013).

Mobile payments. Mobile payments differ from mobile banking which merely provides a mobile interface or method for accessing traditional bank accounts and services from a financial institution. Mobile payments do not theoretically require a bank account (Suárez, 2016). Mobile payments can be conducted directly between two mobile users in a peer-to-peer (P2P) model or between a mobile user and a retailer or business. Many mobile payments services allow users to perform transactions using the Short Message Service (SMS) text messaging protocol. Funds can either be pre-funded or settled through a mobile network operator's standard billing process (Choo, 2013).

Mobile payments pose many of the same money laundering risks as prepaid cards. Multiple funding channels, potentially anonymous funding channels, cash withdrawals, and a lack of familiarity with customer due diligence requirements by many mobile service providers all present significant AML risk. The provisioning of mobile payment services may also be highly segmented to include mobile network operators, distributors, and electronic money issuers (Financial Action Task Force, 2013).

Internet-based payments. Internet-based payment services represent the broadest category of NPPS. Per the FATF, Internet-based payment services provide pre-funded accounts that permit the transfer of value via the Internet. These services include digital wallets, digital currencies, virtual currencies and electronic money. However, the continuously evolving world of NPPS makes it difficult to definitively classify these products and services. The interaction between prepaid card, mobile payment and Internet-based payment technologies further complicates any attempt to conclusively define a NPPS service or product (Financial Action

Task Force, 2013). In fact, the Wolfsberg Group combines mobile and Internet-based payments into a single category that they define as "new and innovative payment products and services which involve different ways of initiating payments through, or extending the reach of, traditional retail electronic payment systems, as well as products that do not rely on traditional systems to transfer value" (The Wolfsberg Group, 2014, p. 3, para. 2).

Internet-based payment services are vulnerable to all the same money laundering risks as prepaid cards and mobile payment services. Due to the many variations of products and services that could be considered Internet-based payments, the risks are often more pronounced. Internet-based payments services rarely involve face-to-face contact with customers, may be funded via third-parties and exchanges that further obscure the source of funds, and are often global in reach. Even though Internet-based payment services typically do not provide customers with direct access to cash, the anonymity, obfuscation, and geographical reach provided by these products present many money laundering risks (Financial Action Task Force, 2013).

The Importance of Mexico

The late Cameron "Kip" Holmes (2014), a recognized expert in AML, former chief of the Financial Remedies Section of the Arizona Attorney General's Office, and former Director of the Southwest Border Anti-Money Laundering Alliance, warned that the collapse of the Mexican economy was imminent if the dominance of organized crime groups over the same was not abated in the short term. As the United States' third-largest trading partner, a failure of the Mexican economy would have disastrous effects on the economy of the entire North American region. Improving Mexico's money laundering prevention efforts could make a significant impact on reducing organized crime in the country and contribute to avoiding the predicted economic collapse (Holmes, 2014). Even if Holmes has overstated the likelihood of pending

economic doom, Mexico remains an important piece of the world economy. Mexico is currently the world's fifteenth-largest economy and estimated to become the fifth-largest by 2050 (Department for International Trade, 2016). Further, Mexico is the fourth-largest recipient of remittance funds globally, receiving $25.7 billion in 2015 (The World Bank, 2016).

Paradoxically, and despite the global importance of the Mexican economy, the use of formalized financial services in the country is low when compared to other countries in the region. Perception surveys demonstrate that in Mexico there is a lack of trust in traditional financial institutions and antipathy towards the high costs associated with maintaining traditional accounts (Alonso, Fernández de Lis, Hoyo, López-Moctezume, & Tuesta, 2013). At the same time, the demand for financial services in the country is high (Suárez, 2016). The Mexican economy suffers from low levels of financial inclusion (Del Angel, 2016).

The lack of access to financial services and participation in the formal financial sector, known as financial exclusion, is a hindrance to economic development and growth. Conversely, financial inclusion has been shown to offer many benefits including reducing rates of illness and unemployment. On a macro-level, financial inclusion reduces poverty, reduces inequality and stabilizes the economy (Flores-Roux & Mariscal, 2010). Policy makers in Mexico have demonstrated a desire to improve the country's level of financial inclusion. In 2015, Mexico joined 60 other countries in signing the Maya Declaration of Financial Inclusion pledge, promoting financial inclusion through means that include new and innovative financial services (Del Angel, 2016). NPPS, including prepaid cards, mobile payment services and Internet-based payment services, are viewed as catalysts for promoting increased financial inclusion (The Wolfsberg Group, 2011; The Wolfsberg Group, 2014).

The Challenge to Mexico

Mexico's own Financial Intelligence Unit estimates that nearly nine billion dollars were laundered through the Mexican economy between 2007 and 2012 (Behrens, 2015). The United States Department of State has designated Mexico as a Country of Primary Concern for money laundering. This designation was given largely due to the drug trafficking income that may be laundered through the Mexican economy. Other factors contributing to this designation include the significant impact of the informal economy and Mexico's geographical location between the United States and Central America. Money laundering techniques utilized in Mexico traditionally included cross-border currency smuggling and trade-based money laundering. Additionally, with the cash-related restrictions implemented in 2010, money laundering methods have shifted towards less cash-intensive means, increasing the reliance on trade-based schemes (United States Department of State, 2016).

After early struggles to correct failures identified in a 2008 Anti-Money Laundering and Combating the Financing of Terrorism Mutual Evaluation, Mexico had sufficiently addressed the identified primary areas of concern by February of 2014. The progress made by Mexico towards improving the country's AML measures was significant and has led to the country's removal from the follow-up process to which it was subject to for nearly seven years (Financial Action Task Force, 2014a). The changes to Mexico's AML regime, especially the passing of new legislation in 2012 and its implementation in 2013, have been generally lauded as a success (Financial Action Task Force, 2014a; Behrens, 2015). A significant increase in money laundering related prosecutions has earned the country high marks, yet concerns remain regarding the country's emphasis on prevention over enforcement (Behrens, 2015). Of particular importance for this research was the inclusion of defined vulnerable activities, including the

issuance of prepaid cards, as subject to specified AML regulations under the Federal Law for the Prevention and Identification of Operations with Resources of Illicit Origin of 2012 (Arteaga, 2014). This paper explored AML measures in Mexico as they relate to NPPS to provide an understanding of Mexico's preparedness to combat the threats to its economy posed by money laundering both in the present and future. Throughout this research the pressure of expanded use of NPPS in Mexico was contemplated as a stress test which would either validate or repudiate Mexico's AML regime and the progress made towards improving the country's money laundering prevention measures.

Literature Review

This project sought to enumerate the money laundering risks presented by NPPS, discover strategies and measures that can be implemented by a country to combat the money laundering risks posed by NPPS, and assess whether NPPS are adequately covered within Mexico's AML regulatory framework. In seeking to determine whether Mexico's AML measures are sufficient to respond to the challenges presented by NPPS, this research reviewed recent academic literature, industry participant reports, international organization guidance and the relevant laws, regulations and directives. The literature review was divided into three sections corresponding to the primary questions posed by this research project.

Money Laundering Risks of New Payment Products and Services

The first aspect addressed in this research project was the money laundering risks presented by NPPS. The literature available regarding the money laundering risks of new payment products and services is composed primarily of reports and guidance developed by international, non-governmental organizations. Additionally, industry advocates and participants, such as the GSM Association, discussed the risks presented by NPPS within their specific

industry. Lastly, a scholarly article by Kim-Kwang Raymond Choo reviewed the money laundering risks of NPPS in multiple countries utilizing FATF mutual evaluation results.

Financial Action Task Force research. The FATF is an international, inter-governmental organization that promotes the implementation of AML and counter terrorist financing measures. The FATF authors and maintains a list of recommendations, known as the Forty Recommendations, which set standards for national AML measures (See Appendix A). In addition to coordinating and setting methodology for mutual evaluations of participating countries, the FATF issues reports and guidance on subjects of importance to policy makers and financial institutions (Financial Action Task Force, 2012).

In 2006 the FATF issued an initial report on NPPS to raise consciousness of the potential abuse of these products and services by money launderers. The outcome of that report recommended that a more detailed update be conducted after a few years of further study. The follow-up report in 2010 analyzed more than 30 case studies provided by member countries and survey responses to develop common money laundering typologies, risk factors and common risk characteristics of NPPS. Before addressing the money laundering risks of NPPS, the report highlighted the opportunities for financial crime prevention presented by these products and services. The opportunities relate to the potential of NPPS to replace the use of cash and illegal transactions conducted through unregulated financial services. Despite the anonymity provided by many NPPS, these products and services nearly universally create some electronic record, however minimal, which does not always exist in purely cash transactions (Financial Action Task Force, 2010).

While the functionalities of NPPS vary greatly between different products, services and providers, the 2010 FATF report identified three overarching characteristics of NPPS that

present risk. First, the absence of credit risk for NPPS (the products and services are commonly prepaid) does not provide much incentive for providers to gather full customer information, which would otherwise be required for potential future collection efforts and could be further utilized for transaction monitoring and customer due diligence purposes. Second, the value proposition of many NPPS includes the speed by which transactions can be conducted. By the time any suspicious activity is detected, the funds have likely already been converted to another form and cannot be detained. Third, most NPPS do not require any in-person interaction, increasing the potential for abuse and the presentation of falsified information when customer identifying information is collected. The report then categorized NPPS risk factors into customer due diligence, record keeping, value limits, methods of funding, geographical limits, usage limits and segmentation of services groups (Financial Action Task Force, 2010). Each of the categories and the related risk factors detailed in the report are summarized in the following paragraphs.

Regarding customer due diligence, the 2010 FATF report signaled anonymity as a primary risk factor of NPPS. Anonymity can be a risk of any type of NPPS, especially since customer contact is often limited or non-existent. In the case of Internet-based payment services, customer relationships are rarely established in-person which further enhances the anonymity of the product. In the case of prepaid cards, proper identification of the initial customer may not be enough to limit the anonymity risk as cards can be transferred physically and easily to unknown third-parties. For any type of NPPS, even when a provider collects customer data, poor verification of a customer's identity can create a further potential risk factor. Collecting a customer's name and identifying information may not be sufficient if the veracity of the information cannot be validated using independent sources. In some countries that lack a national

identity framework, such as a unique voter identification or social security numbering scheme, customer identity verification can be especially difficult (Financial Action Task Force, 2010).

Regarding methods of funding, the 2010 FATF report lists anonymous funding, third-party funding, indirect funding, and multiple sources of funding as potential risk factors. Anonymous funding occurs when no or limited information is gathered regarding the funder or origin of funds. Third-party funding occurs when an individual other than the customer provides the funds for the NPPS account. Similarly, indirect funding can occur when a NPPS provider allows funds to be put into an account via a P2P transaction, potentially avoiding source of fund controls. Finally, another risk factor related to the method of funding NPPS is allowing an account to be funded from multiple sources or via multiple channels. A combination of these factors without sufficient controls could cause a product or service to be considered high risk for money laundering (Financial Action Task Force, 2010).

The 2010 FATF report covers both value limits and usage limits as risk categories related to NPPS. Products or services with no limits or high limits regarding the maximum amounts that can be stored on an account, the maximum amounts per transaction and transaction frequency all present higher risk. The report also notes that customer due diligence requirements may potentially be linked to value limits in such a way that those customers who provide more information are granted higher limits. Similarly, a lack of usage limits represents a risk factor. Higher negotiability translates to higher risk. A product or service that can only be carried out between customers of the same provider is less risky than a product or service that allows payments through a wide variety of merchants or networks (Financial Action Task Force, 2010).

The final three risk categories mentioned in the 2010 FATF report are geographical limits, segmentation of services, and record keeping. Regarding geographical limits, the report

only lists one risk factor which is the geographical reach of the product or service. NPPS that are negotiable in multiple geographies imply higher risks than those which are limited to domestic payments only. The report presents open-loop prepaid cards as a specific example, noting that cards which are negotiable via global ATM networks provide opportunities to move funds across multiple jurisdictions quickly. Regarding segmentation of services, the report discusses how multiple providers involved in differentiated aspects of the payment product or service create opportunities for loss of information and lack of accountability. Increased segmentation of services creates additional complexity and therefore higher risk. Regarding record keeping, most NPPS providers create some sort of digital record, but the value of that data may vary. The FATF addresses record keeping in Recommendation 10 (updated to Recommendation 11 in 2012), but does not explicitly require the collection of IP addresses. Nonetheless, collecting and recording IP addresses related to NPPS can reduce record keeping risk (Financial Action Task Force, 2010).

In a June 2014 report, the FATF focused on the money laundering risks of virtual currencies, a subset of the Internet-based payment services NPPS category. The report described risk factors already covered in previous FATF reports on NPPS, but provided further detail and definition as related to the virtual currencies (Financial Action Task Force, 2014b). First, the report defined a virtual currency as "...a digital representation of value that can be digitally traded..., but does not have legal tender status in any jurisdiction" (Financial Action Task Force, 2014b, p. 4, para. 2). The key aspect of this definition is the lack of legal tender status which differentiates virtual currency from e-money (also a form of NPPS) which is simply the digital representation of a recognized currency, such as the U.S. Dollar, British Pound or Mexican Peso. Although the term digital currency was often used ambiguously in previous FATF reports, the

2014 report defined digital currency as an overarching term that covers both virtual currency and e-money. Virtual currencies may either be convertible in that they can be directly or indirectly exchanged for other recognized, fiat currencies, or non-convertible in that they are limited to use within a defined digital environment. Of the two types, only convertible virtual currencies present risks of money laundering. Non-convertible virtual currencies are limited to their defined environment and do not interact with the larger economy which significantly reduces any risk posed. Nonetheless, the FATF warns that the definitions of convertible and non-convertible are fluid and the development of a black market for a non-convertible virtual currency would effectively render that virtual currency as convertible (Financial Action Task Force, 2014b).

Virtual currencies can be further subdivided as centralized (controlled by a single administrative authority) or decentralized (P2P without a central authority). The decentralized virtual currencies, such as Bitcoin, are the most vulnerable to the risks of anonymity, as no central authority is tasked with collecting customer identification information. Further complicating the situation is that Bitcoin, a prominent virtual currency, was designed not to attach any customer identifying information to accounts known as Bitcoin addresses nor transactions. It is exceedingly difficult for regulators and law enforcement to apply regulations and provide oversight of decentralized virtual currency schemes that lack of a single authority. The remaining risks defined in the 2014 FATF report on virtual currencies mirror those discussed in the 2010 FATF on NPPS, such as anonymous funding, third-party funding, lack of face-to-face customer relationship, global negotiability and segmentation of services (Financial Action Task Force, 2014b).

Wolfsberg Group guidance. The Wolfsberg Group is an affiliation of thirteen international banks, including Banco Santander, Bank of America, Bank of Tokyo-Mitsubishi

UFJ, Barclays, Citigroup, Credit Suisse, Deutsche Bank, Goldman Sachs, HSBC, J.P. Morgan Chase, Société Générale, Standard Chartered Bank, and UBS. The group's mission is to provide AML and counter terrorist financing related guidance (The Wolfsberg Group, 2015). The organization addressed the money laundering risks of NPPS in two different guidance documents published in 2011 and 2014. The 2011 *Wolfsberg Guidance on Prepaid and Stored Value Cards* notes many of the same money laundering risk factors mentioned in the 2010 FATF report, but with a focus on the risks presented by prepaid cards. The 2011 Wolfsberg Group guidance additionally presented risks specific to prepaid cards that are not applicable to other NPPS (The Wolfsberg Group, 2011). The 2014 *Wolfsberg Guidance on Mobile and Internet Payment Services (MIPS)* describes many of the same money laundering risk factors mentioned in the 2010 FATF report and the 2011 Wolfsberg Group guidance, but with a focus on the risks presented by mobile and Internet-based payment services. The 2014 Wolfsberg Group guidance additionally reviewed risks specific to mobile and Internet-based payment services that are not applicable to other NPPS (The Wolfsberg Group, 2014).

In the 2011 prepaid card guidance, the Wolfsberg Group noted that prepaid cards are the most utilized of all NPPS. The guidance echoed the 2010 FATF report in detailing risks related to prepaid cards, including the potential lack of geographical limitations of the product, the potential lack of customer due diligence, the potential of funding through cash or cash equivalents, the potential of funding from third-parties, the potential lack of funding limits, the potential to withdraw funds in cash, and the potential for high segmentation of service providers. The 2011 Wolfsberg Group guidance addressed additional risk factors not mentioned in the 2010 FATF report that belong to the risk categories of anonymity, geographical scope, product users, and value term limits. Related to anonymity, prepaid cards do not typically provide a useful audit

trail and because they may be negotiable by an unidentified bearer, monitoring of aggregate activity by a user is difficult or impossible. In regards to the geographical scope, prepaid cards that are negotiable globally can be intentionally utilized in countries known to have weak AML laws. In regards to product users, prepaid cards present increased money laundering risk when there is no control over the use of the account by multiple users. Value term limits are the final additional risk category of factors not discussed in the 2010 FATF report. The 2011 Wolfsberg Group guidance notes that prepaid cards with limited terms may be less appealing to money launderers and therefore products with no expiration date pose increased risk. Additionally, the guidance expanded on the 2010 FATF report risk category of segmentation of service providers by defining the maximum number of distinct roles in prepaid card distribution and use to be a total of nine. Finally, the guidance highlighted that non-bank service providers often play a role in the distribution and use of prepaid cards and pose money laundering risk when they are not regulated or are regulated to a lower standard than banks (The Wolfsberg Group, 2011).

In the 2014 mobile and Internet-based payment services guidance, the Wolfsberg Group repeated many of the money laundering risks to NPPS mentioned in both the 2010 FATF report and the 2011 Wolfsberg Group guidance on prepaid cards, including the potential lack of geographical limitations of the product, the potential lack of customer due diligence, the potential of funding through cash or cash equivalents, the potential of funding from third-parties, the potential lack of funding limits, the potential lack of value term limits, the potential to withdraw funds in cash, and the potential for high segmentation of service providers. The 2014 Wolfsberg Group guidance on mobile and Internet-based payment services followed the 2011 Wolfsberg Group guidance on prepaid cards by noting that non-bank service providers often play a role in the distribution and use of mobile and Internet-based payment services and pose money

laundering risk when they are not regulated or are regulated to a lower standard than banks. The 2014 Wolfsberg Group guidance concluded by calling for better definition of terminology related to prepaid cards, mobile payment systems and Internet-based payment services (The Wolfsberg Group, 2014).

Industry perspectives. Industry participants have provided insight, and sometimes counter-arguments, regarding the potential money laundering risks of NPPS. The GSM Association (GSMA), a mobile communications industry and standards setting group, published a discussion paper in 2010 regarding assessing the risks of money laundering and terrorist financing from mobile payment services. The research was prefaced on the benefits that mobile payment services provide to developing countries and unbanked populations (Solin & Zerzan, 2010). The authors considered only those mobile payments which fall under the umbrella of NPPS so that the paper excluded from discussion "convenient means of access to a bank account" (Solin & Zerzan, 2010, p. 11, para. 3). GSMA and the authors acknowledged that mobile payment services do present money laundering risks related to the anonymity, traceability and rapidity offered, but held that except for rapidity, these risks were less severe than the same features of cash payments. The risk of anonymity for mobile payment services occurs when a country does not require face-to-face registration for services. The fact that registration of some sort is required signifies that the risk of anonymity with mobile payment systems is less than with cash. Mobile payments, by their nature, are traceable and therefore far less elusive than cash transactions. However, because mobile payments can be instantaneous they do pose a significant risk related to their rapidity. The paper also noted the possibilities of money laundering through mobile payment services in the case of complicit providers or third party agents. The positions of trust and knowledge held by these entities would allow them to falsify records or ignore

suspicious behavior. Finally, it was noted that unregulated, mobile payment services would pose a systemic risk to economies. Nonetheless, if proper oversight is in place, the use of mobile payment systems reduces the overall money laundering risks faced by an economy as it displaces high risk and difficult to monitor cash payments (Solin & Zerzan, 2010).

Some experts in virtual currency contend that the money laundering risks of these products and services are often overstated by organizations such as the FATF and the Wolfsberg Group. Juan Llanos, a recognized leader in the areas of virtual currency, Bitcoin, and AML regulation, once declared that "Bitcoin was born regulated" (Marty, 2014, para. 3). In addition to serving as a member of the Bitcoin Foundation's regulatory affairs committee, Mr. Llanos has also worked as an anti-money laundering advisor at Coinalytics and was the Chief Compliance and Transparency Officer for Bitreserve. Mr. Llanos has stated that the commonly held beliefs that Bitcoins are anonymous, untraceable, and invisible to law enforcement, are in fact myths. Despite the presence of money laundering related risks, the fear of virtual currencies is largely overstated and misses the opportunities afforded for financial crime prevention by the adoption of this technology, such as the ability for direct investigation by authorities and suspicious activity detection of published transactions (Llanos, 2016).

Mr. Llanos' statements represent more than an industry expert's opinion as they are supported by technical research. A study at the University College Dublin in Dublin, Ireland has demonstrated that multiple technological and analytical techniques may be applied to the analysis of Bitcoin transaction history, which is publicly available, in order to associate activity with identifying information (Reid & Harrigan, 2012). Furthermore, the authors of the study countered claims of the lack of traceability among decentralized virtual currencies such as Bitcoin when they noted that "With appropriate tools, the activity of known users can be

observed in detail" (Reid & Harrigan, 2012, p. 26, para. 2). Another study, conducted principally by graduate students at the University of California, San Diego, also concluded that Bitcoin does not provide complete anonymity, especially if there is a need to convert the value to fiat currency. The industry is controlled by a relatively limited number of exchanges, all transactions are publicly visible, and methods exist allowing identification of flows of funds (Meiklejohn et al., 2013). The authors of the study argue that these limitations "make Bitcoin unattractive today for high-volume illicit use such as money laundering" (Meiklejohn, et al., 2013, para. 6).

Academic perspectives. Kim-Kwang Raymond Choo provided a framework for analyzing a country's susceptibility to money laundering and terrorist financing risks from NPPS. Choo focused his analysis and review on stored value prepaid cards and mobile money transfer systems. Choo first identified the FATF recommendations that apply to new payment methods and then utilized FATF mutual evaluations and follow-up reports to assess the strength of multiple countries' AML regimes as related to NPPS. The relevant FATF recommendations included Special Recommendation VI (money or value transfer services; updated to Recommendation 14 in 2012), Recommendation 8 (new technologies; updated to Recommendation 15 in 2012), and Recommendation 20 (other measures; dispersed among other recommendations in the 2012 update). Choo's research found that countries which did not require licensing or registration of money and value transfer services would often receive ratings of Non-Compliant for Special Recommendation VI. Countries whose legislation lacked requirements for the implementation of risk mitigating policies related to relationships that were not established in person could expect a poor rating for Recommendation 8. Although Recommendation 20 potentially represented the broadest of the recommendations reviewed in Choo's research, it was also the recommendation with the highest level of compliance among the

countries reviewed. Only one of the 65 countries evaluated received a rating of Compliant for all three recommendations reviewed – Hungary (Choo, 2013). Choo noted that countries with low levels of compliance, in particular with regard to Special Recommendation VI and Recommendation 8, "could potentially create a [favorable] situation for criminals and terrorists looking to infiltrate the global financial system" (Choo, 2013, p. 22, para. 1). Although his analysis did not include the country of Mexico, the framework and methodology presented could be utilized to evaluate any country that has undergone an FATF mutual evaluation (Choo, 2013).

Mitigating Money Laundering Risks of New Payment Products and Services

Before determining if Mexico's AML regulatory framework successfully addresses the money laundering risks of NPPS, this project necessitated a review of the strategies and measures that a country may implement to combat the risks previously discussed. The literature available surrounding the mitigation of the money laundering risks of NPPS included FATF guidance, a GSMA research paper, and academic research projects. The principal topics discussed within the literature concerning the mitigation of the money laundering risks of NPPS include the promotion of risk assessments for designing money laundering controls, defining the entities subject to money laundering measures, the recommended money laundering controls themselves, and the need for the designation of competent supervisory authorities.

Excessive regulation and risk assessments. Much of the literature surrounding the mitigation of the money laundering risks of NPPS also cautioned against excessive or restrictive regulation that could have detrimental effects on other initiatives, such as efforts to improve financial inclusion. The literature also universally recommended the application of a risk-based approach to the implementation of money laundering controls for NPPS.

In 2013, the FATF built upon the research conducted and published in their 2010 report regarding the potential for abuse of NPPS. The 2013 FATF *Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services* detailed the organization's views on how governments can address the money laundering risks of NPPS. Although the report was focused on risk mitigation measures, the FATF believed it necessary to mention that overly conservative approaches towards implementing AML measures may have the opposite effect desired by setting the barriers for legitimate NPPS providers and users so high that they are forced to utilize underground services beyond the supervision of regulators, further exacerbating the concerns that the measures would seek to address. Therefore, the FATF called for risk assessments to be conducted related to NPPS prior to the implementation of regulations and controls. The adopted measures should be proportionate to the risks presented. The report highlights the importance of Recommendation 15 (classified as Recommendation 8 prior to 2012) of the FATF Recommendations which requires that countries and private institutions evaluate the money laundering risks of new products and technologies (Financial Action Task Force, 2013).

The additional available literature supports the 2013 FATF guidance. In a research project sponsored by the Centre for International Finance and Regulation (CIFR), the University of New South Wales (UNSW), Standard Chartered Bank, and the United Nations Capital Development Fund (UNCDF), the FATF's endorsement of risk based approaches was repeated. The authors encouraged regulators to lead the efforts to promote financial inclusion through the implementation of proportional regulation of NPPS. Overly conservative regulatory approaches adopted by regulators whose sole goal is to comply with the FATF Recommendations and earn satisfactory marks on an FATF mutual evaluation may inadvertently limit economy development

and financial inclusion (Malady, Buckley, & Arner, 2014). In an analysis of the mobile payments industries in the Philippines and Kenya and of the effect of AML regulations in these countries, William Vlcek emphasized "the need for regulation and supervision of mobile technologies, while maintaining recognition of the development and social-welfare opportunities from the use of mobile telephones and m-money as a payments system in a developing economy" (Vlcek, 2011, p. 426, para. 2).

The GSMA advocates for allowing both mobile network operators and traditional financial institutions to offer mobile payment services. Citing examples of countries that require the involvement of banks in the provision of mobile payment services, the association notes that these forced partnerships may limit customer adoption due to a conservative application of money laundering controls without applying a risk-based approach. The GSMA, in agreement with the Bank for International Settlements (BIS), therefore recommends that regulations be applicable based on the activity or type of services offered instead of by the institution that offers them (di Castri, 2013).

Entities Subject to Regulation. The money laundering controls recommended by the reviewed literature and summarized in the next section would be irrelevant if a country is unable to impose the requirements on the proper providers of the product or service. As presented in previous sections, segmentation of services among multiple roles in the provision of NPPS complicates efforts to mitigate the money laundering risks posed (Financial Action Task Force, 2010; The Wolfsberg Group, 2011; The Wolfsberg Group, 2014).

The 2013 FATF guidance states generally that NPPS providers should be subject to regulation. In regards to determining which entity in a segmented provision scheme should be designated as the provider and therefore subject to AML regulation, the FATF recommends that

focus be placed on entities which manage the NPPS, entities responsible for maintaining customer relationships, entities that receive funds, or entities against which a customer would be able to make a claim for the funds in question. It is also possible for more than a single entity within an NPPS scheme to be subject to regulation. In the case of prepaid cards, the FATF signals the card issuer as the most appropriate entity to be subject to regulation. In the case of mobile payment services, the FATF signals the bank or mobile network operator that manages the funds as the entity that ought to be subject to regulation. In the case of Internet-based payment services, the FATF signals that the entity that manages relationships with customers should be subject to regulation (Financial Action Task Force, 2013).

Additionally, the 2013 FATF guidance instructs countries to subject NPPS providers to licensing, registration, and the adoption of money laundering control measures when the provider meets the definition of a money or value transfer service (MVTS) as defined by the FATF Recommendations (Financial Action Task Force, 2013). The glossary of the FATF Recommendations defined MVTS as follows:

> financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs. (Financial Action Task Force, 2012, p. 122)

Finally, the 2013 FATF guidance clarifies that Internet-based payment services, despite potentially being outside of the traditional jurisdiction of a country's financial regulations, should be submitted to the same requirements as other NPPS providers offering products or services within the country (Financial Action Task Force, 2013).

In the case of virtual currencies, a more specific answer to the question of which entities ought to be regulated is provided by Dr. Robert Stokes, a lecturer at the Liverpool Law School of the University of Liverpool. Dr. Stokes contends that as the gateways between virtual currency and legal tender fiat currencies, the entities that conduct exchange of virtual currencies, such as Bitcoin, for government-backed currencies, should be subject to money laundering control measures and responsibilities. A virtual currency that cannot enter the real economy does not pose serious money laundering risks. In most countries, a framework for the regulation of traditional currency exchanges already exists into which virtual currency exchanges could be incorporated (Stokes, 2013). Others concur with Stokes and believe that the most logical entities to regulate in the world of Bitcoin are the currency exchanges. Furthermore, these exchanges provide an efficient focal point for law enforcement (Bryans, 2014).

Money laundering controls. The potential controls that countries may require for NPPS providers to implement to mitigate money laundering risks, and proposed within the literature, can be divided into the categories of customer due diligence, activity limits, record keeping requirements, transaction monitoring and reporting, and agent oversight. While controls such as those discussed in the following sections are essential to mitigate the risks of a product or service being utilized for money laundering, the FATF also cautioned against taking a universal approach to their application. The FATF instead advocates for a risk-based application of money laundering controls which would force a country to evaluate the potential risks of each product or service. To promote financial inclusion, the FATF has recommended that controls be applied according to a principle of proportionality, in which required controls are proportional to the risk presented by a given product or service (Financial Action Task Force, 2013).

Customer due diligence. Customer due diligence has been highlighted throughout the literature as a key measure that regulators should require of NPPS providers for mitigating the risks of money laundering. The practice typically consists of customer identification, verification, and monitoring processes. The 2013 FATF guidance holds that in accordance with the results of risk assessments, simplified or reduced customer due diligence controls may be applied for NPPS or customers considered to be low risk. Tiered customer due diligence requirements should be proportional to the risk presented by the NPPS or customer, and may even be greater than those required of other traditional products and services, such as when in-person customer verification is not possible. Requirements could be placed such that when cash is utilized as a source of funding for an NPPS account, enhanced due diligence is required on the individuals providing the funds. Additionally, NPPS providers should be required to conduct ongoing customer due diligence on accounts and perhaps may be required to update due diligence information upon the occurrence of other trigger events such as the re-loading of an NPPS account (Financial Action Task Force, 2013).

The other literature reviewed supports the FATF's recommendations related to risk based customer due diligence requirements. The establishment of tiered identification requirements alleviates the need to conduct risk assessments that imagine every potential product or service (Malady, Buckley, & Arner, 2014). Customer due diligence requirements can be simplified, especially when other supplemental controls are implemented (di Castri, 2013). While acknowledging the potential that simplified customer due diligence requirements may attract money launderers to products and services utilizing these reduced requirements, Malady, Buckley, and Arner called for regulators to promote simplified customer due diligence among NPPS providers. Technological advances may improve identification techniques, thereby

reducing the risk factors which customer due diligence seeks to mitigate. However, regulation requiring customer due diligence should be technology-independent to allow for these advances (Malady, Buckley, & Arner, 2014).

Activity limits. Limiting various aspects of a product or service can render them less attractive tools to money launderers and effectively reduce the money laundering risk of NPPS. Limits can be placed on nearly all aspects of a product or service, including limitations on the amount that may be loaded, limitations on the number of times value may be loaded, limitations on the transferring of funds between users, limitations on the maximum amounts that may be held on account, limitations on the maximum amount of payment, limitations on the frequency of cash withdrawals, and limitations on the geographical access to accounts. Additionally, limits could be tiered in conjunction with the customer due diligence program such that customers could be required to provide more information to gain access to less restrictive limits (Financial Action Task Force, 2013). By focusing on the intended customer of a given service, sensible money laundering controls may be implemented. This was the case in both Kenya and the Philippines where mobile payment services were utilized primarily by low-income customers who regularly sent smaller value payments. Limiting transactions to lower value amounts allows the service to meet customer needs yet mitigates the risk of money laundering by reducing the service's attractiveness as a method for laundering large amounts of money (Vlcek, 2011).

Record keeping requirements. NPPS providers should be required, at a minimum, to maintain records of payments that include any identifying information collected regarding the payer and payee, the date of the transaction, the amount of the transaction, and accounts utilized. The FATF recommends that transaction records be kept without respect to the value of the transaction or transactions in question. The organization additionally recommends all related

information, including transaction records and customer due diligence information be maintained for no less than five years (Financial Action Task Force, 2013).

Transaction monitoring and reporting. The 2013 FATF guidance recommends that countries impose transaction monitoring and suspicious activity reporting requirements on NPPS providers, regardless of the determined risk of a given product or service. In fact, the guidance outlines the increased importance of this measure in the face of limited customer identification means (Financial Action Task Force, 2013). Transaction monitoring can also complement activity limits to discover structured transactions conducted by money launderers attempting to avoid activity restrictions (di Castri, 2013).

Agent oversight. The use of third-party distributors via an agent relationship is particularly common in the provision of prepaid cards and mobile payment services. The agents may be held responsible for complying with AML measures, but the NPPS provider itself should monitor the compliance of the agents with the applicable measures (Financial Action Task Force, 2013). Providers should also be held responsible and liable for the actions of third-parties working on their behalf as a method to motivate providers to conduct sufficient third-party oversight and due diligence. Finally, providers should be required to deliver training to third-parties distributing products and services on their behalf (di Castri, 2013).

Supervisory authorities. The designation of competent supervisory authorities to oversee and monitor NPPS providers is essential to mitigating the money laundering risks of NPPS. The 2013 FATF guidance recommends the countries assign a single supervisory authority responsible for oversight of all NPPS providers for compliance with AML measures, even if this implies supervision across multiple sector or industries. When this is not possible, or practical, channels for communication between supervisory authorities with responsibility for NPPS

providers should be established. If a country decides to appoint an agency as a supervisory authority that does not traditionally oversee compliance with AML measures, such as a telecommunications authority, it is necessary that sufficient education and training are provided to that agency (Financial Action Task Force, 2013).

Anti-Money Laundering Measures in Mexico

The final question this project sought to answer was whether Mexico's AML regulatory framework sufficiently addresses the money laundering risks of NPPS and implements recommended strategies to mitigate those risks. An evaluation of Mexico's AML legislation and related regulatory framework was conducted for subsequent comparison with the recommended mitigation measures. The literature available surrounding the AML measures in Mexico includes the relevant legislation, FATF mutual evaluations, and a scholarly article.

Legislative Framework. The first step in evaluating Mexico's anti-money laundering regime was to directly review and analyze the relevant legislation. The present section summarized the relevant legislation, including the Federal Law for the Prevention and Identification of Operations with Resources of Illicit Origin. The section also examined relevant rulings and interpretative advisories of the regulatory authority.

Criminalization of Money Laundering. Articles 400 Bis and 400 Bis 1 of Mexico's Federal Penal Code (Código Penal Federal [CPF]) criminalized money laundering. Article 400 Bis of the CPF criminalized the acts of acquiring, administering, converting, depositing, investing or transferring resources which are known to be proceeds of illegal activity. Additionally, the act of concealing or attempting to conceal the nature or source or ownership of resources which are known to be proceeds of illegal activity was criminalized. Article 400 Bis 1 of the CPF augments the applicable penalties when these acts are committed by individuals who

are employees of regulated institutions or by individuals who are public functionaries. (Congreso de la Unión, 2014a).

Money or Value Transfer Services. Article 95 Bis of Mexico's General Law of Auxiliary Credit Organizations and Activities (Ley General de Organizaciones y Actividades Auxiliares del Crédito [LGOAAC]) governs money transmitters and currency exchangers, under which some NPPS providers may be classified. Section 1 of Article 95 Bis of the LGOAAC establishes the primary responsibilities of the regulated entities to include developing measures to prevent the activity that had been criminalized under Article 400 Bis of the CPF. Section 2 of Article 95 Bis of the LGOAAC requires the presentation of reports regarding detected criminal activities to the designated government authority (Congreso de la Unión, 2014b).

The Secretariat of Finance and Public Credit (Secretaría de Hacienda y Crédito Público [SHCP]) issued General Orders referring to Article 95 Bis of the LGOAAC (Disposiciones de carácter general a que se refiere el artículo 95 Bis de la Ley General de Organizaciones y Actividades Auxiliares del Crédito [DCG]) which outlined additional responsibilities for money transmitters and currency exchangers. Order 49 of the DCG requires that money transmitters establish measures to ensure that authorized agents offering their products or services are complying with all relevant obligations. Order 49 also requires that the money transmitter conducts due diligence on all authorized agents offering their products or services. Section 1 of Order 50 of the DCG specifically denotes that money transmitters are ultimately responsible for the compliance of authorized agents with the measures and controls established within the law. Finally, the entirety of Chapter 6 of the DCG is dedicated to the reporting of unusual or suspicious activity (Secretaría de Hacienda y Crédito Público, 2012).

The Federal Anti-Money Laundering Law. In July of 2013 Mexico's Federal Law for the Prevention and Identification of Operations with Resources of Illicit Origin (Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita [LFPIORPI]) came into effect. The law's accompanying Statement of Intent, as presented to the Senate, outlined the motives for, and necessity of a new AML regime in the country. Notably, prior to the implementation of the LFPIORPI, only financial institutions were subject to AML requirements by means of supervisory regulations that were dispersed throughout 11 different laws governing each category of financial institution. The supervisory regulations were issued by the SHCP, but did not have the force of a law enacted by a legislative body. The LFPIORPI unified the dispersed laws under a single legal structure and further included non-financial institutions as regulated entities based on the vulnerability of the organization's activity. To complement this requirement, the LFPIORPI defined a specific list of denominated vulnerable activities, including the issuance of prepaid cards and instruments utilized in a payment system. Additionally, Article 15 of the law establishes record keeping requirements related to customer due diligence and Article 19 provides for simplified compliance requirements, including customer due diligence, for activities considered to be low-risk. Article 32 prohibits the use of cash in specified transaction types, however the transaction types listed in the law were not related to NPPS (Congreso de la Unión, 2012).

The SHCP published the implementing regulations accompanying the LFPIORPI (Reglamento de la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita [RLF]) on August 16 of 2013 with an effective date of September 1 of 2013. The RLF generally reflected and reinforced the provisions of the LFPIORPI. The RLF further clarified vague provisions of the LFPIORPI, provided details regarding calculations of

sums for reporting, and defined the methods by which the affected entities should comply with the provisions of the law. Articles 21 through 31 of the RLF delineated and further defined the vulnerable activities that cause an institution to become regulated (Secretaría de Hacienda y Crédito Público, 2013a).

Additionally, procedural rules to the LFPIORPI were issued by the SHCP on August 23 of 2013, modified on July 24 of 2014, and a clarification of the modification issued on July 31 of 2014. The rules and their clarifications in their entirety are known as the General Rules referred to by LFPIORPI (Reglas de Carácter General a que se refiere la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita [RCG]). The rules are technical in nature and provide greater detail than either the law or regulation. Annex 1 of the RCG details the specific elements of information for customer identification measures that must be collected for customers that are physical persons. Annex 2 of the RCG details the specific elements of information for customer identification measures that must be collected for customers that are legal entities. For the application of simplified measures and controls, Article 34 of the RCG enables providers of vulnerable activities to define criteria for classification of customers and users as low risk, based on the best practices and guides as distributed by the country's Financial Intelligence Unit (Unidad de Inteligencia Financiera [UIF]). For low risk customers or users, providers are required to collect the reduced list of elements for customer identification measures as listed in Annexes 3, 4, 4 Bis, 5, 6, 6 Bis, 7 Bis or 8 of the RCG, depending on customer or user attributes (Secretaría de Hacienda y Crédito Público, 2013b).

Regulatory Authorities and Supervisory Agencies. Within the LFPIORPI, multiple agencies and institutions are designated with various levels of authority and responsibilities for the regulation and supervision of the law. Article 5 of the LFPIORPI designated the SHCP as the

authority responsible for the administration of the law. Article 6 of the LFPIORPI enumerated the emission of regulations pursuant to the law as one of the responsibilities of the SHCP. Article 7 of the LFPIORPI ordered the creation of a specialized financial analysis unit within the office of the Attorney General (Procuraduría General de la República [PGR]). Finally, Article 16 designated the National Banking and Securities Commission (Comisión Nacional Bancaria y de Valores [CNBV]), the National Insurance and Surety Commission (Comisión Nacional de Seguros y Fianzas [CNSF]), and the Tax Administration Service (Servicio de Administración Tributaria [SAT]) as the authorities responsible for the supervision and verification of compliance of financial institutions throughout the country (Congreso de la Unión, 2012).

Rulings and Interpretations. As stated in the preceding section, the SHCP was granted the power to issue relevant regulations and administer the law under the agencies executive authority (Congreso de la Unión, 2012). By this authority and through the agency's Money Laundering Prevention Portal (Portal de prevención de lavado de dinero), the SHCP publishes advisories and interpretations. Of importance to this research project, a September of 2015 advisory clarified the regulatory agency's interpretation of the LFPIORPI with respect to virtual currency. In said advisory, the SHCP referenced the FATF 2014 guidelines related to virtual currencies and clarified that Article 32 of the LFPIORPI (cash restrictions) will apply to virtual goods. The advisory defined virtual goods as data stored in information systems that can be transmitted electronically, and that although not legal currency in any jurisdiction, is utilized as a means of exchange, to conduct commerce, or to make payments. Lastly, the advisory explicitly excluded from the definition of virtual goods, those digital units which are utilized only in gaming platforms or loyalty programs, and limited to use with the issuer of the specified units or affiliated businesses (Secretaría de Hacienda y Crédito Público, 2015).

Financial Action Task Force Mutual Evaluations. Mexico was evaluated for compliance with the FATF Recommendations in 2004 and again in 2008. The 2008 mutual evaluation was conducted using the 2004 FATF Mutual Evaluation Methodology which utilized the FATF 40 Recommendations plus 9 Special Recommendations framework. The 2008 evaluation noted progress made since the previous evaluation in 2004, but still highlighted the need for improvement. Mexico's money laundering prevention measures allowed for risk-based application by financial institutions, yet fell short in other areas. Of the 49 recommendations evaluated, Mexico received the following ratings: Compliant (C) for seven recommendations; Largely Compliance (LC) for seventeen recommendations; Partially Compliant (PC) for nineteen recommendations; and, Non-Compliant (NC) for six recommendations (See Appendix B). As related to NPPS, Partially Compliant ratings were given for Recommendation 5 (customer due diligence; updated to Recommendation 10 in 2012), Recommendation 8 (new technologies; updated to Recommendation 15 in 2012), and Special Recommendation VI (money or value transfer services; updated to Recommendation 14 in 2012). Additional concerns were noted regarding the effectiveness of the country's institutions dedicated to investigating and prosecuting money laundering related crimes (Financial Action Task Force, 2008).

As part of the mutual evaluation process, Mexico received follow-up evaluations in October of 2010, October of 2011, October of 2012, February of 2013, June of 2013, and October of 2013. The follow-up evaluations reviewed the progress of the Mexico towards improving in areas rated as Partially Compliant or Non-Compliant. In the seventh and final follow-up report, Mexico had made sufficient progress in correcting the evaluated deficiencies and requested termination of the follow-up process. The implementation of the LFPIORPI was a major factor in addressing the deficiencies discovered during the 2008 mutual evaluation. The

deficiencies related to Recommendation 5 (customer due diligence; updated to Recommendation 10 in 2012) were remedied by the implementation of new regulations. Stricter customer due diligence requirements were put in place in 2009 and amended in 2012. Additionally, guidance was provided regarding the applicability of simplified customer due diligence. Although, not considered key recommendations, Mexico reported making progress on both Recommendation 8 (new technologies; updated to Recommendation 15 in 2012) and Special Recommendation VI (money or value transfer services; updated to Recommendation 14 in 2012). New requirements created an obligation to identify clients in advance of conducting any transaction and strict cash deposit limits have been imposed in which customer identification requirements trigger at relatively low amounts for these transactions. Lastly, the report declined to make an evaluation regarding the effectiveness of the institutions dedicated to investigating and prosecuting money laundering offenses, but noted that the number of money laundering related prosecutions have increased over the years evaluated (Financial Action Task Force, 2014a).

Academic Perspectives. The literature also demonstrated that Mexico's efforts to strengthen money laundering prevention measures may have had negative impacts on its efforts to improve financial inclusion. Sandra Suárez, a Political Science professor at Temple University, authored a comparative study of mobile payment services in the countries of Kenya and Mexico. Suárez found that despite low access to traditional financial services and high adoption of mobile phone technology in both countries, only 2.2% of the population of Mexico utilized mobile payment services as compared to 57.1% of the population of Kenya (Suárez, 2016). In 2015, Mexico's Federal Commission for Economic Competition (Comisión Federal de Competencia Ecónomica) noted that only 2.6 million out of 100 million cellular phone service subscribers held a mobile bank account (Bibian, 2015). Suárez found that a primary cause of this

disparity was the different regulatory approaches observed in each country in regards to mobile payments (Suárez, 2016). Suárez noted the following:

> The regulatory dilemma is whether or not to treat mobile money as mobile banking, and require money users to open a bank account and provide the same documentation they would be required by a bank, when the benefits of mobile money are that users can take advantage of the service at a lower cost with the technology they already possess. (Suárez, 2016, p. 5, para. 2)

In the case of Mexico, mobile payment services may only be offered in conjunction with a traditional banking institution. Although these services are permitted to utilize simplified low-risk account types for reduced customer due diligence, the regulatory requirements that necessitate the involvement of traditional financial institutions in the provision of mobile payment services have limited the service's penetration within Mexico (Suárez, 2016).

A 2014 report by the Alliance for Financial Inclusion (AFI) compared the regulatory frameworks covering mobile financial services in six Latin American countries. Bolivia, Colombia, Paraguay, and Peru all allow, or are in the process of considering laws that would allow participation in the provision of mobile financial services by non-bank entities. In Mexico and Guatemala, however, mobile payments services can only be provided by banks or regulated financial institutions. The AFI report coincides with the information presented by Suárez and further noted that the requirements for bank involvement in the provision of mobile financial services in Mexico originate from various regulations and rulings emitted by Mexico's Central Bank (Banco de México [Banxico]), the SHCP, and the CNBV (Alliance for Financial Inclusion, 2014).

Discussion of the Findings

This research project sought to analyze AML measures implemented in Mexico to assess the preparedness of the country to respond to the threat of abuse of NPPS. The following questions were answered through research conducted as part of this project: What are the money laundering risks presented by new payment products and services? What strategies and measures can be implemented by a country to combat the money laundering risks posed by new payment products and services? Are new payment products and services contemplated and covered by Mexico's AML regulatory framework?

Authoritative literature and primary sources (legislation, regulations, and rulings) demonstrated that Mexico's AML measures adequately address the money laundering related risks of NPPS. The breadth of Mexico's current AML measures covers and regulates all potential NPPS providers. The depth of Mexico's current AML measures encompasses the potential money laundering related risks of NPPS. Additionally, the research showed that Mexico's current AML measures may be excessively restrictive for NPPS providers, particularly in the subcategory of mobile payments. The research conducted led to the development of the themes discussed in the following paragraphs.

Breadth of Mexico's Anti-Money Laundering Measures for NPPS

The first area of analysis in this research project was to determine whether all possible providers of NPPS were contemplated within Mexico's laws and regulations. This was defined as the breadth of Mexico's AML measures related to NPPS. The research found that all current types of NPPS are contemplated within Mexico's AML regime and providers of such are considered regulated entities.

The issuance and sale of prepaid cards by non-financial institutions are designated as vulnerable activities by Article 17, Section 2 of the LFPIORPI. The sale of prepaid cards for an amount equivalent to or greater than 645 times the minimum salary of the Federal District of Mexico City is subject to reporting to the SHCP. Financial institutions that participate in the issuance or sale of prepaid cards (or participate in any other designated vulnerable activity) are regulated under Article 15 of the LFPIORPI and the corresponding law established to govern the specific type of financial institution (Congreso de la Unión, 2012). Article 23 of the RLF clarified that reloading or further deposit after issuance of prepaid cards is also a covered activity as contemplated within the law (Secretaría de Hacienda y Crédito Público, 2013a). The LFPIORPI and RLF extend coverage of providers of prepaid cards to both non-financial institutions and financial institutions that provide this product. Prepaid card providers, regardless of their designation as a financial institution, are therefore subject to regulation within the breadth of Mexico's anti-money laundering measures.

The provision of mobile payment services by non-financial institutions is not permitted in Mexico. Instead, all such payments are conducted via partnerships between mobile phone service providers and established financial institutions, such as banks, or in a model involving only the financial institution (Suárez, 2016). All forms of recognized financial institutions are regulated under Article 15 of the LFPIORPI and the corresponding law established to govern the specific type of financial institution (Congreso de la Unión, 2012). Therefore, mobile payment providers, as established financial institutions, are subject to regulation within the breadth of Mexico's anti-money laundering measures.

Article 22, Section 2 of the RLF designated the provision of stored value instruments, including electronic wallets, as vulnerable activities that are regulated per Article 17, Section 2

of the LFPIORPI. The issuance or sale of these products or services for an amount equivalent to or greater than 645 times the minimum salary of the Federal District of Mexico City is subject to reporting to the SHCP (Secretaría de Hacienda y Crédito Público, 2013a). Financial institutions that participate in the provision of electronic stored value instruments (or participate in any other designated vulnerable activity) are regulated under Article 15 of the LFPIORPI and the corresponding law established to govern the specific type of financial institution (Congreso de la Unión, 2012). Further, through the organization's rulemaking and advisory powers, the SHCP clarified that virtual currencies are covered goods within the definitions of Article 32 of the LFPIORPI (Secretaría de Hacienda y Crédito Público, 2015). The LFPIORPI and RLF extend coverage of providers of Internet-based payments to the both non-financial institutions and financial institutions that provide these services. Internet-based payment providers, regardless of their designation as a financial institution, are therefore subject to regulation within the breadth of Mexico's AML measures.

While the breadth of Mexico's AML measures, in particular the LFPIORPI and RLF, appear to provide sufficient coverage of potential providers of NPPS, the definition of NPPS is broad and the variety of products and services that could be considered NPPS, especially within the Internet-based payments category, is growing. The speed of growth of potential NPPS could quickly outpace the government's ability to legislate amendments to the LFPIORPI or implement a new legislative scheme contemplating previously unaddressed areas. However, as evidenced by the SHCP's issuing of a ruling regarding virtual currencies, the LFPIORPI is sufficiently flexible to adapt to risks which are yet unforeseen (Secretaría de Hacienda y Crédito Público, 2015).

Depth of Mexico's Anti-Money Laundering Measures for NPPS

After evaluating whether Mexico's laws and regulations covered all possible providers of NPPS (breadth), this study sought to evaluate whether the money laundering risks of NPPS (depth) were adequately mitigated by the country's AML measures. By comparing the money laundering controls that NPPS providers are required to implement in the country with the controls designated within the literature as necessary to mitigate the risks, this research discovered that after the legislative reforms and the implementation of the LFPIORPI, Mexico is largely prepared to address the money laundering risks of NPPS. Nonetheless, the AML measures implemented in Mexico fell short in regards to the risks of NPPS in three categories. The money laundering controls discussed in the literature were grouped into five categories: customer due diligence, activity limits, record keeping requirements, transaction monitoring and reporting, and agent oversight.

The money laundering control category of customer due diligence is fully addressed in Mexico's AML measures. The obligations of institutions that participate in vulnerable activities (of which NPPS providers are included) are described in Article 18 of the LFPIORPI. Sections 1 and 2 of Article 18 provide for customer due diligence requirements such as identification of customers and users, verification of identification through official documentation and credentials, and the solicitation of information regarding clients' professional activities. Additionally, Article 19 of the LFPIORPI allows for the establishment of simplified compliance requirements based on risk (Congreso de la Unión, 2012). Article 15 of the RLF put forward that the specific terms and conditions of applying simplified compliance measures would be established in general rules emitted by the SHCP (Secretaría de Hacienda y Crédito Público, 2013a). However, Article 34 of the RCG allowed each provider of vulnerable activities to

establish their own criteria for defining customers as high or low risk (Secretaría de Hacienda y Crédito Público, 2013b).

The money laundering control category of activity limits is only partially addressed in Mexico's AML measures. The LFPIORPI designates an activity limit related to the use of cash in defined transaction types, yet none of those transaction types, as listed in the law, are related to NPPS (Congreso de la Unión, 2012). The cash restriction provision was expanded by the SHCP in a ruling that included virtual goods (Secretaría de Hacienda y Crédito Público, 2015). Otherwise, the LFPIORPI does not generally impose limits on specific product activity such as a limit on the value that may be loaded onto a prepaid card. Instead, the LFPIORPI defines the activity amounts for the defined vulnerable activities at which an entity must provide transaction and client information to the SHCP (Congreso de la Unión, 2012). Providers that wish to avoid the obligations and associated costs to comply with the reporting requirements may opt to impose limits on the products and services they offer to remain below the defined thresholds.

Despite the lack of NPPS specific activity limits (except for limits on the cash purchase of virtual goods), the allowance of simplified customer due diligence requirements may impose an indirect activity limit above which a customer must present further verification documentation. Article 34 of the RCG dictates that each provider of vulnerable activities will establish their own criteria to define customers or users as high or low risk per best practices published by the country's FIU and the risks posed by the specific activity (Secretaría de Hacienda y Crédito Público, 2013b). Providers of NPPS could consider those risk factors mentioned by FATF in their guidance, and therefore base the criteria and risk factors for simplified customer due diligence on those discussed throughout this research project. Providers evaluating risk factors related to account load amounts, withdrawal or transfer amounts, account

balance limits, or geographic access would place activity limits on the product or service. Other than the cash restrictions related to virtual goods, no law, regulation, or rule directly imposes activity limits on providers of NPPS and any such risk clarification is largely left to the discretion of the provider.

The money laundering control category of record keeping requirements is fully addressed in Mexico's AML measures. Article 18, Section 4 of the LFPIORPI requires providers of vulnerable activities to maintain records related to those transactions and customer files for a period of five years from the date of the relevant transaction (Congreso de la Unión, 2012). Article 20 of the RLF requires providers of vulnerable activities to maintain the records related to vulnerable activities for a period of five years from the date of providing the report to the SHCP (Secretaría de Hacienda y Crédito Público, 2013a). The difference in requirements between the LFPIORPI and RLF is minimal and represents the lag between the occurrence of the transaction and the reporting of such to the authorities.

The money laundering control category of transaction monitoring and reporting is only partially addressed in Mexico's AML measures. Although transaction monitoring and reporting of suspicious transactions is required of money transmitters and currency exchange providers, there are no provisions requiring the implementation of a similar control by non-financial institutions that offer vulnerable activities. As not all providers of NPPS will necessarily be money transmitters or currency exchange providers, this disparity represents an area of concern regarding the preparedness of Mexico to address the risks of money laundering from NPPS. The deficiency is mediated in some degree by the requirement of non-financial institution providers of vulnerable activities to report transaction and client data to the SHCP. Article 27 of the RCG requires notice be made to the UIF within 24 hours of receiving knowledge of transaction funds

which are derived from or destined to be part of a crime (Secretaría de Hacienda y Crédito Público, 2013b). This requirement implicitly requires at least a minimal level of monitoring of transactions conducted, but is very vague compared to the explicit monitoring requirements imposed on money transmitters and currency exchangers. Additionally, in theory, the specialized financial analysis unit within the PGR created by Article 7 of the LFPIORPI should be monitoring and reviewing the transaction data to which they have access (Congreso de la Unión, 2012).

The money laundering control category of agent oversight is only partially addressed in Mexico's AML measures. NPPS providers that are regulated money transmitters are held liable and responsible for the actions of agents offering their services under Order 49 of the DCG. Nonetheless, NPPS providers that are not traditional financial institutions are not covered by the DCG (Secretaría de Hacienda y Crédito Público, 2012). The providers that are covered by the provisions of LFPIORPI for vulnerable activities would not be explicitly held to this requirement.

The analysis conducted throughout this research paper discovered that all NPPS types were contemplated within the AML measures implemented in Mexico (breadth). The analysis also revealed that all the AML measures implemented in Mexico either fully addressed or partially addressed all the controls necessary to mitigate the risks of NPPS (depth). The author developed a chart to show both the breadth and depth of the AML measures implemented in Mexico (See Appendix C). The chart further indicates the provisions of the laws, regulations, and rules which cover or partially cover each control. Many of these measures did not exist until the 2013 implementation of the LFPIORPI.

Proportionality of Mexico's Anti-Money Laundering Measures for NPPS

Although the research has shown that Mexico has implemented many AML measures to sufficiently address the potential risks posed by NPPS, the research has also indicated that some measures may go too far. Concerns exist that regulations which would limit the use of NPPS may unintentionally and negatively impact a nation's attempt to improve the level of financial inclusion (Financial Action Task Force, 2013). In some cases, Mexico has adopted the concept of proportionality, such as in the measures allowing institutions to conduct simplified customer due diligence for lower risk products and customers. Nonetheless, in the case of mobile payments, by requiring the involvement of a bank or other established financial institution, Mexico has severely limited the growth of this service. The demographic numbers and measures of demand show that the service could be potentially as popular as in Kenya where 57.1% of the population utilize mobile payment services as of 2013 (Suárez, 2016). This requirement is particularly perplexing considering the Mexican government's desire to improve the rate of financial inclusion as evidenced by the country becoming a signatory to the Maya Declaration of Financial Inclusion (Del Angel, 2016). Additionally, with the implementation of the LFPIORPI, Mexico has taken steps to focus regulations on activities considered to be vulnerable instead of exclusively regulating financial institutions (Congreso de la Unión, 2012). This regulatory model could be applied to mobile payments offered by non-financial institutions. The LFPIORPI's applicability to various non-financial institutions based on the products and services engaged in, instead of the type of institution offering the product or service, has shown that Mexico could successfully implement AML measures that mitigate the risk of NPPS which at the same time are not overly onerous to the point of damaging financial inclusion related initiatives.

Comparison of Findings with Existing Studies

There have been no other studies conducted which directly address whether the legislative and regulatory measures of Mexico sufficiently prepare the country for the potential money laundering risks posed by the introduction of NPPS. Kim-Kwang Raymond Choo's research looked at multiple countries' compliance with three FATF Recommendations as determined by the author to be the most relevant recommendations related to risks posed by NPPS (Choo, 2013). Although Choo provides an excellent baseline framework for evaluating a country's ability to address NPPS related risks, it did not consider all the possible risks as revealed throughout the remaining literature. Additionally, Choo's study did not consider the country of Mexico. After the regulatory reforms undertaken by the country, Mexico would be considered compliant with the three FATF Recommendations reviewed by Choo. The broad nature of FATF Recommendations, such as those utilized in Choo's study, is therefore only appropriate when seeking a general understanding of the preparedness of a group of countries in relation to the money laundering risks posed by NPPS. For these reasons, the present study included a more nuanced and detailed analysis of the identified money laundering risks of NPPS as compared to the relevant legislation in Mexico.

Limitations of the Study

This research project confirmed the overall preparedness of Mexico to address the money laundering risks of NPPS from a legislative and regulatory perspective. Nonetheless, the data reviewed placed doubt on the effectiveness of the institutions charged with enforcing the relevant laws and those responsible for prosecuting money laundering offenses. Commentators in the literature highlighted the increase in prosecutions in the country as evidence that it has made significant improvements regarding enforcement (Behrens, 2015). While the percentage increase

in prosecutions is substantial, the difference in real numbers reveals that Mexico still does not prosecute many cases of money laundering each year (See Appendix D). Without proper enforcement and vigilant prosecution of money laundering offenses, many of the controls which NPPS providers are required to implement are rendered irrelevant. Controls such as value limits can be effective regardless of prosecutorial diligence, however; other controls such as transaction monitoring and suspicious activity reporting are intended to provide law enforcement with information and are only effective in deterring money laundering if the threat of prosecution is present. It is not clear whether the limited enforcement is due to poor performance within the country's FIU, lack of political will to prosecute within the Attorney General's office, or some other reason.

Recommendations

This research project was conducted to discover if Mexico was prepared to address and respond to the threat of money laundering utilizing NPPS. The literature reviewed identified the money laundering risks of NPPS as well as measures that may be taken by countries and institutions to mitigate these risks. The literature also demonstrated that there is some disagreement as to the level of risks posed by NPPS and highlighted concerns regarding the possibility of negative impacts to financial inclusion efforts if NPPS are excessively regulated. The literature reviewed included primary sources such as the relevant laws, regulations, rulings and orders issued by the country's legislature and regulatory bodies. The analysis of the literature revealed that Mexico has implemented measures sufficient to mitigate the risks of money laundering presented by NPPS. While the measures implemented have been assessed as sufficient, a few modest gaps related to the control requirements of NPPS providers were discovered. The subsequent paragraphs describe recommendations for shoring up and

remediating incomplete measures, provide a recommendation for ensuring that other measures do not unnecessarily impair efforts for the improvement of financial inclusion, outline potential areas of future research, and finally present a brief conclusion.

Strengthening the LFPIORPI

The LFPIORPI and its related regulations, rulings, and orders have fortified Mexico's AML measures in regards to non-financial institutions offering defined vulnerable activities, including for NPPS providers. The results of this research project would have been dramatically different prior to the implementation of the LFPIORPI and its related regulations, rulings, and orders. Nonetheless, this research project did observe three control categories in which the AML measures that a country should implement to prevent the misuse of NPPS were only partially addressed in Mexico. The following recommendations focus on strengthening the LFPIORPI in regards to these three control categories and their coverage of NPPS providers that are not financial institutions.

Based upon the findings of the research, the author recommends that the LFPIORPI be amended to include explicit activity limits related to account load limits, withdrawal/transfer limits, maximum account balance limits, and geographic access limits for defined vulnerable activities. As noted in the discussion section, non-financial institutions that provide vulnerable activities (covering non-financial institution NPPS providers) may independently impose activity limits on certain products or customers with the goal of defining these as low-risk and allowing the provider to apply simplified due diligence. However, each provider is responsible for establishing their own criteria to define a customer or product as low-risk (Secretaría de Hacienda y Crédito Público, 2013b). In many cases, activity limits could form part of this rating criteria, but it is not guaranteed within the legislation. To remedy these deficiencies, the

LFPIORPI should be amended to explicitly require activity limits for non-financial institution providers of vulnerable activities. Alternatively, the DCG could be updated to explicitly define the criteria that must be utilized to delineate high- and low-risk accounts instead of leaving it to the provider's discretion and include activity limits within that definition.

The author further recommends that the LFPIORPI be amended to explicitly require transaction monitoring and suspicious transaction reporting of all providers of vulnerable activities, regardless of their status as a financial institution or non-financial institution. As shown, transaction monitoring and suspicious activity reporting are required of NPPS providers that are considered money transmitters or currency exchangers (Secretaría de Hacienda y Crédito Público, 2012). For all other providers, Article 27 of the RCG may implicitly require transaction monitoring, but that will ultimately be a question of regulator interpretation (Secretaría de Hacienda y Crédito Público, 2013b). To eliminate doubt and strengthen this control, the LFPIORPI should be amended to explicitly require transaction monitoring and suspicious activity reporting by non-financial institution providers of vulnerable activities.

To strengthen the LFPIORPI and based upon the findings of the research, the author additionally recommends that the LFPIORPI be amended to include liability for actions taken by agents of non-financial institutions that participate in vulnerable activities. As with the other recommendations provided, the control category of agent oversight and provider liability for agent actions is only contemplated for regulated NPPS providers that are considered money transmitters or currency exchangers (Secretaría de Hacienda y Crédito Público, 2012). Any NPPS providers that are not financial institutions are not subject to any specific agent oversight requirements. The LFPIORPI should be amended to include strict liability for providers that utilize agents if any of those agents violate any of the provisions of the law.

Permitting the Mobile Payments Industry to Expand

To ensure that the goal of financial inclusion is not adversely impacted by excessive regulation, the author recommends that mobile phone networks be allowed to provide mobile payment services without the requirement that the service be linked to a bank account provided by a regulated financial institution. Mexico's LFPIORPI shifted the country's AML framework from focusing on institutions to a more inclusive regulation based on activity type (Congreso de la Unión, 2012). By requiring that mobile payment services be offered in partnership with defined banking institutions and deposit accounts, Mexico has potentially limited the expansion of these services. Given the expanded coverage of AML regulation via the LFPIORPI, the rulings requiring involvement of banking institutions in the provision of mobile payment services, as issued by Banxico, the SHCP, and the CNBV, should be reversed to support efforts aimed at the improvement of financial inclusion. Further, if the previous recommendations to strengthen the LFPIORPI are implemented, the country should feel even more secure in allowing mobile payments to be classified as vulnerable activities and regulated despite being offered by non-financial institutions.

Future Research Required

According to the findings of the research conducted, the money laundering risks of NPPS have been largely addressed throughout Mexico's legislation. Nonetheless, the literature reviewed exposed a potential gap in regards to the enforcement of this legislation. No previous study has specifically examined the enforcement of Mexico's AML measures as related to NPPS. Further research is required to quantify and evaluate the enforcement of Mexico's AML regime in relation to the risks posed by NPPS.

Additionally, this project considered only those products and services currently defined as NPPS, with a specific adherence to the categories defined by the FATF including prepaid cards, mobile payments, and Internet-based payments (Financial Action Task Force, 2013). It is possible that new, innovative, and unforeseen products or services emerge that present risks which were not considered within this analysis. To ensure that Mexico's AML legislative measures and required controls account for these potential future products and services, academics and government officials must constantly evaluate the risk landscape. Future periodic research is needed to repeat the analysis conducted within this project and update the literature upon which it relied.

Finally, although this research project focused on the country of Mexico, the evaluation of the breadth and depth of the country's AML measures is a repeatable process. The framework developed to evaluate Mexico's preparedness for responding to the money laundering risks of NPPS has expanded upon the substantial related works of others, such as Kim-Kwang Raymond Choo (Choo, 2013). The author of the present study intended to enhance the research previously conducted by others and provide a framework which could be applied to any country. Further research ought to independently assess and evaluate the relevance of this proposed framework, as well as apply it to other countries.

Conclusions

This research project endeavored to discover the money laundering risks of NPPS, elaborate the measures that a country should implement to mitigate those risks, and finally to compare the AML legislation of Mexico with those recommended measures to determine whether the country was prepared to address the money laundering risks of a growing and likely to be important NPPS sector. The outcome of the research project was to find that Mexico is

prepared to respond to the threat of abuse of NPPS for the purposes of money laundering. Mexico has made many enhancements to their AML regime and legislative framework which have led to this conclusion. The LFPIORPI of 2013 and its related regulations, rulings, and orders have had a significant impact in addressing the risks of NPPS.

To initiate the research, literature was reviewed which enumerated the money laundering risks of NPPS, described the controls necessary to mitigate the money laundering risks of NPPS, and the AML measures implemented in the country of Mexico. The first section of the literature review discovered the money laundering risks of NPPS by reviewing reports and guidance developed by international, non-governmental organizations, and articles written by industry participants. The second section of the literature review identified the controls necessary to mitigate the money laundering risks of NPPS by reviewing FATF guidance, an industry research paper, and academic research projects. The third and final section of the literature review explored the AML measures in place in Mexico by reviewing relevant legislation, FATF mutual evaluations, and a scholarly article.

Following the literature review, an analysis was conducted that first examined the breadth, or NPPS product and service coverage, of the Mexican AML legislation. Of the three major categories of NPPS, both prepaid cards and Internet-based payments were regulated under the LFPIORPI. In the case of mobile payments, this service was prohibitively offered only in partnership with major banks or otherwise regulated financial institutions and therefore would be covered under previous AML laws and regulations. The analysis then looked at the depth, or controls required of NPPS providers, of the Mexican AML legislation. Of the five major control categories, Mexico's legislation fully addresses all aspects of two categories and partially addresses aspects of three categories. No aspect or category was insufficiently addressed nor

completely unaddressed within the legislation. In the case of the partially addressed control categories, most deficiencies discovered were related to controls that existed implicitly or were left to regulator interpretation. In the case of agent oversight requirements, however; neither an implicit nor explicit control existed for non-financial institutions.

Despite the author's conclusion that Mexico is prepared to address the money laundering risks of NPPS, the literature review also revealed concerns regarding the burdensome requirement to work with traditional financial institutions on mobile payment providers. As a country that is dedicated to improving its level of financial inclusion, Mexico must find the right balance of regulation that will prevent money laundering without debilitating efforts to provide financial services to everyone. The LFPIORPI advanced the country's money laundering prevention measures and increased the regulation surrounding non-financial institutions, yet did not create excessive burdens and even allowed for the application of new simplified customer diligence procedures for low-risk customers and products (Congreso de la Unión, 2012). Nonetheless, existing rulings by multiple agencies prevented mobile phone networks from providing mobile payment solutions without the involvement of a traditional financial institution (Alliance for Financial Inclusion, 2014). This research project recommended that these rulings be reversed and for the allowance of mobile payment services untethered to traditional financial institutions.

The goals of this research project of determining the preparedness of Mexico to address the money laundering risks of NPPS and evaluating the control measures required by legislation and regulation for that purpose were accomplished. Nonetheless, the study was limited in that it did not evaluate the enforcement of these measures. Legislative and regulatory measures are nothing more than words on a page if they are not enforced and therefore the final success of the

great efforts undertaken to enhance the country's AML measures depends on complementary enforcement efforts. Further research should be conducted to quantify and evaluate the enforcement of Mexico's AML regime in relation to the risks posed by NPPS.

The author also put forth recommendations, based upon the findings of the research, to strengthen the areas of the LFPIORPI that were determined to only partially address the money laundering risks of NPPS. First, the LFPIORPI should be amended to explicitly require activity limits on non-financial institution providers of NPPS. Second, the LFPIORPI should be amended to explicitly require transaction monitoring and suspicious activity reporting of non-financial institution providers of NPPS. Lastly, the LFPIORPI should be amended to include strict liability for NPPS providers that utilize agents if any of those agents violate any of the provisions of the law. Implementing these changes would fortify the relatively comprehensive AML legislative and regulatory measures of Mexico.

References

Alliance for Financial Inclusion. (2014). *Enfoques regulatorios para los servicios financieros móviles en Latinoamérica.* Bangkok.

Alonso, J., Fernández de Lis, S., Hoyo, C., López-Moctezume, C., & Tuesta, D. (2013, June). Mobile banking in Mexico as a mechanism for financial inclusion: recent developments and a closer look into the potential market. *BBVA Research: Working Papers*. Mexico City.

Arteaga, J. R. (2014, January 1). El ABC para cumplir con la Ley Anti-Lavado. *Forbes Mexico*. Retrieved from http://www.forbes.com.mx/el-abc-para-cumplir-con-la-ley-anti-lavado/#gs.3=YwBJo

Behrens, T. (2015). Lift-off for Mexico? Crime and finance in money laundering governance structures. *Journal of Money Laundering Control, 18*(1), 17-33.

Bibian, C. (2015, July 20). Banca móvil sin movimiento. *MILENIO*. Retrieved from http://www.milenio.com/negocios/ftmercados-Banca_Movil-BBVA_Bancomer-_negocios_0_556744389.html

Bryans, D. (2014). Bitcoin and Money Laundering: Mining for an Effective Solution. *Indiana Law Journal, 89*(1), 441-472.

Choo, K.-K. R. (2013, July). New payment methods: A review of 2010-2012 FATF mutual evaluation reports. *Computers & Security, 36*, 12-26.

Congreso de la Unión. (2012, October 17). Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita [Federal Law for the Prevention and Identification of Operations with Resources of Illicit Origin].

Congreso de la Unión. (2014a, March 14). Código Penal Federal [Federal Penal Code].

Congreso de la Unión. (2014b, January 10). Ley General de Organizaciones y Actividades Auxiliares de Crédito [General Law of Auxiliary Credit Organizations and Activities].

Del Angel, G. A. (2016, May). Cashless Payments and the Persistence of Cash: Open Questions About Mexico. *Hoover Institution Economics Working Papers*. Stanford, California.

Department for International Trade. (2016, May 10). *Doing business in Mexico: Mexico trade and export guide*. Retrieved from GOV.UK: https://www.gov.uk/government/publications/exporting-to-mexico/exporting-to-mexico

di Castri, S. (2013, February). *Mobile Money: Enabling regulatory solutions.* GSMA.

Financial Action Task Force. (2008, October 17). *Mutual Evaluation Report: Anti-Money Laundering and Combating the Financing of Terrorism: Mexico.* Paris. Retrieved from http://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20Mexico%20ful.pdf

Financial Action Task Force. (2010, October). *Money Laundering Using New Payment Methods.* Paris. Retrieved from http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf

Financial Action Task Force. (2012, February). *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations.* Paris. Retrieved from http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

Financial Action Task Force. (2013, June). *Prepaid Cards, Mobile Payments and Internet-Based Payment Services: Guidance for a Risk-Based Approach.* Paris. Retrieved from http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf

Financial Action Task Force. (2014a, February). *Mutual Evaluation of Mexico: 7th Follow-Up Report.* Paris. Retrieved from http://www.fatf-gafi.org/media/fatf/documents/reports/mer/Follow-up-report-Mexico-2014.pdf

Financial Action Task Force. (2014b, June). *Virtual Currencies: Key Definitions and Potential AML/CFT Risks.* Paris. Retrieved from http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

Flores-Roux, E. M., & Mariscal, J. (2010, June 2015). The Enigma of Mobile Money Systems. *Communications and Strategies*, 41-62.

Harrup, A. (2016, January 1). Mexican E-Commerce Grows, but Requires Some Coaxing. *The Wall Street Journal*. Retrieved from http://www.wsj.com/articles/mexican-e-commerce-grows-but-requires-some-coaxing-1451683541

Holmes, C. H. (2014). *Organized Crime in Mexico: Assessing the Threat to North American Economies.* Potomac Books.

Laya, P. (2015, March 12). Mexican Vendors Bypass Banks With Mobile Applications. *Bloomberg Technology*. Retrieved from http://www.bloomberg.com/news/articles/2015-03-12/mexican-vendors-bypass-banks-with-mobile-applications

Llanos, J. (2016, October 4). Bitcoin, Blockchains & Financial Crime presentation at Verafin FRAMLxpo. Grapevine, TX.

Malady, L., Buckley, R., & Arner, D. (2014, June). Developing and Implementing AML/CFT Measures using a Risk-Based Approach for New Payments Products and Services. Centre for International Finance and Regulation Research Papers. Retrieved from

http://www.uncdf.org/sites/default/files/Documents/using_a_risk-based_approach_for_aml_cft_measures_for_new_payment_technologies_june_2014.pdf

Marty, B. (2014, December 12). Juan Llanos: “Bitcoin Was Born Regulated”. *PanAm Post*. Retrieved from https://panampost.com/belen-marty/2014/12/12/juan-llanos-bitcoin-was-born-regulated/

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2013). A fistful of bitcoins: characterizing payments among men with no names. *Proceedings of the 2013 conference on Internet measurement conference* (pp. 127-140). New York: Association of Computing Machinery.

Reid, F., & Harrigan, M. (2012, May 7). An Analysis of Anonymity in the Bitcoin System. Retrieved from https://arxiv.org/abs/1107.4524

Secretaría de Hacienda y Crédito Público. (2012, April 10). Disposiciones de Carácter General a que se refiere el artículo 95 Bis de la Ley General de Organizaciones y Actividades Auxiliares del Crédito.

Secretaría de Hacienda y Crédito Público. (2013a, August 16). Reglamento de la Ley Federal para la Prevención e Identifiación de Operaciones con Recursos de Procedencia Ilícita.

Secretaría de Hacienda y Crédito Público. (2013b, August 23). Reglas de Carácter General a que se refiere la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita.

Secretaría de Hacienda y Crédito Público. (2015, September). Aviso Importante: Respecto a la utilización de activos virtuales en los actos u operaciones establecidos en el artículo 32 de la ley federal para la prevención e identificación de operaciones con recursos de

precedencia ilícita (LFPIORPI). *Portal de prevención de lavado de dinero*. Retrieved from https://sppld.sat.gob.mx/pld/index.html

Solin, M., & Zerzan, A. (2010, January). Mobile Money Methodology for Assessing Money Laundering and Terrorist Financing Risk: GSMA Discussion Paper. GSMA.

Stokes, R. (2013). Anti-Money Laundering Regulation and Emerging Payment Technologies. *Banking & Financial Services Policy Report, 32*(5), 1-10.

Suárez, S. L. (2016, March 31). Poor people's money: The politics of mobile money in Mexico and Kenya. *Telecommunications Policy*.

The Wolfsberg Group. (2011). *Wolfsberg Guidance on Prepaid and Stored Value Cards.* Retrieved from http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg_Guidance_on_Prepaid_and_Stored_Value_Cards_Oct_14,_2011.pdf

The Wolfsberg Group. (2014). *Wolfsberg Guidance on Mobile and Internet Payment Services (MIPS).* Retrieved from http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg-Group-MIPS-Paper-2014.pdf

The Wolfsberg Group. (2015). *Global Banks: Global Standards*. Retrieved from Wolfsberg AML Principles: http://www.wolfsberg-principles.com/

The World Bank. (2016). *Migration and Remittances Factbook 2016.* Global Knowledge Partnership on Migration and Development (KNOMAD).

United States Department of State. (2016, March). *International Narcotics Control Strategy Report: Money Laundering and Financial Crimes.* Bureau for International Narcotics and Law Enforcement Affairs.

Vlcek, W. (2011, July). Global Anti-Money Laundering Standards and Developing Economies: The Regulation of Mobile Money. *Development Policy Review, 29*(4), 415-431.

Wladawsky-Berger, I. (2016, June 24). FinTech and Financial Inclusion. *The Wall Street Journal*. Retrieved from http://blogs.wsj.com/cio/2016/06/24/fintech-and-financial-inclusion/

Appendices

Appendix A – Financial Action Task Force (FATF) Recommendations

2012 #	2003 #	Recommendation Title
A – AML/CFT POLICIES AND COORDINATION		
1	--	Assessing risks & applying a risk-based approach
2	31	National cooperation and coordination
B - MONEY LAUNDERING AND CONFISCATION		
3	1; 2	Money laundering offence
4	3	Confiscation and provisional measures
C - TERRORIST FINANCING AND FINANCING OF PROLIFERATION		
5	SR II	Terrorist financing offence
6	SR III	Targeted financial sanctions related to terrorism & terrorist financing
7	--	Targeted financial sanctions related to proliferation
8	SR VIII	Non-profit organizations
D - PREVENTIVE MEASURES		
9	4	Financial institution secrecy laws
10	5	Customer due diligence
11	10	Record keeping
12	6	Politically exposed persons
13	7	Correspondent banking
14	SR VI	Money or value transfer services
15	8	New technologies
16	SR VII	Wire transfers
17	9	Reliance on third parties
18	15; 22	Internal controls and foreign branches and subsidiaries
19	21	Higher-risk countries
20	13; SR IV	Reporting of suspicious transactions
21	14	Tipping-off and confidentiality
22	12	DNFBPs: Customer due diligence
23	16	DNFBPs: Other measures
E - Transparency and Beneficial Ownership of Legal Persons and Arrangements		
24	33	Transparency and beneficial ownership of legal persons
25	34	Transparency and beneficial ownership of legal arrangements
F - Powers and Responsibilities of Competent Authorities and Other Institutional Measures		
26	23	Regulation and supervision of financial institutions
27	29	Powers of supervisors
28	24	Regulation and supervision of DNFBPs
29	26	Financial intelligence units
30	27	Responsibilities of law enforcement and investigative authorities
31	28	Powers of law enforcement and investigative authorities
32	SR IX	Cash couriers

33	32	Statistics
34	25	Guidance and feedback
35	17	Sanctions
G - International Cooperation		
36	35; SR I	International instruments
37	36; SR V	Mutual legal assistance
38	38	Mutual legal assistance: freezing and confiscation
39	39	Extradition
40	40	Other forms of international cooperation

Note: Financial Action Task Force (FATF) Recommendation Numbers. Adapted from *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations* (pp. 4-5) by Financial Action Task Force, 2012, Paris. Retrieved from http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

Appendix B – Mexico: 2008 FATF Mutual Evaluation Ratings of Compliance

2003 #	Recommendation	Rating
1	Money laundering offence	PC
2	Money laundering offence	LC
3	Confiscation and provisional measures	LC
4	Financial institution secrecy laws	C
5	Customer due diligence	PC
6	Politically exposed persons	LC
7	Correspondent banking	LC
8	New technologies	PC
9	Reliance on third parties	PC
10	Record keeping	C
11	Unusual transactions	LC
12	DNFBPs: Customer due diligence	NC
13	Reporting of suspicious transactions	PC
14	Tipping-off and confidentiality	C
15	Internal controls	LC
16	DNFBPs: Other measures	NC
17	Sanctions	PC
18	Shell banks	LC
19	Other forms of reporting	C
20	Other NFBP & secure transaction techniques	NC
21	Higher-risk countries	LC
22	Foreign branches & subsidiaries	C
23	Regulation and supervision of financial institutions	PC
24	Regulation and supervision of DNFBPs	NC
25	Guidance and feedback	PC
26	Financial intelligence units	LC
27	Responsibilities of law enforcement and investigative authorities	PC
28	Powers of law enforcement and investigative authorities	LC
29	Powers of supervisors	C
30	Resources, integrity, and training	PC
31	National cooperation and coordination	LC
32	Statistics	LC
33	Transparency and beneficial ownership of legal persons	NC
34	Transparency and beneficial ownership of legal arrangements	LC
35	Conventions	LC
36	Mutual legal assistance	LC
37	Dual criminality	LC
38	Mutual legal assistance: freezing and confiscation	PC
39	Extradition	LC
40	Other forms of international cooperation	C

SR I	International instruments	PC
SR II	Terrorist financing offence	PC
SR III	Targeted financial sanctions related to terrorism & terrorist financing	NC
SR IV	Suspicious transaction reporting	PC
SR V	International cooperation	PC
SR VI	Money or value transfer services	PC
SR VII	Wire transfers	PC
SR VIII	Non-profit organizations	PC
SR IX	Cash couriers	PC

Note: Ratings of Compliance with the FATF Recommendations where C = Compliant, LC = Largely Compliant (LC), PC = Partially Compliant, and NC = Non-Compliant (NC). Adapted from *Mutual Evaluation Report – Executive Summary: Anti-Money Laundering and Combating the Financing of Terrorism: Mexico* (pp. 10-21) by Financial Action Task Force, 2008, Paris. Retrieved from http://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20Mexico%20ES.pdf

Appendix C – Breadth and Depth of AML Measures for NPPS in Mexico

		NEW PAYMENT PRODUCTS AND SERVICE TYPES		
		Prepaid Card Providers	*Mobile Payment Providers*	*Internet-based Payment Providers*
	Providers Regulated? (*Breadth*)	✓ (F)	◇ (O)	✓ (M, P)
CONTROLS (*Depth*) ↑ ↓	***CUSTOMER DUE DILIGENCE***			
	Identification and Verification	● (G, H)	◇	● (G, H)
	Tiered/Simplified CDD Requirements	● (J)	◇	● (J)
	ACTIVITY LIMITS			
	Account Load Limits	◉ (N)	◇	◉ (K, N)
	Withdrawal/Transfer Limits	◉ (N)	◇	◉ (N)
	Maximum Balance Limits	◉ (N)	◇	◉ (N)
	Geographic Access Limits	◉ (N)	◇	◉ (N)
	RECORD KEEPING REQUIREMENTS			
	Minimum 5-Year Maintenance	● (I, L)	◇	● (I, L)
	Customer Information Maintenance	● (I, L)	◇	● (I, L)
	Transaction Information Maintenance	● (I, L)	◇	● (I, L)
	TRANSACTION MONITORING & REPORTING			
	Transaction Monitoring	◉ (A, B)	◇	◉ (A, B)
	Suspicious Activity Reporting	◉ (E)	◇	◉ (E)
	AGENT OVERSIGHT			
	Liability for Agent Actions	◉ (C, D)	◇	◉ (C, D)

● Control Fully Addressed
◉ Control Partially Addressed
○ Control Insufficiently Addressed
◇ Not Applicable

Note: Breadth and Depth of AML Measures for NPPS in Mexico, where A = Article 95 Bis, Section 1 LGOAAC (Congreso de la Unión, 2014b); B = Article 95 Bis, Section 2 LGOAAC (Congreso de la Unión, 2014b); C = Order 49 DCG (Secretaría de Hacienda y Crédito Público, 2012); D = Order 50, Section 1 DCG (Secretaría de Hacienda y Crédito Público, 2012); E = Chapter 6 DCG (Secretaría de Hacienda y Crédito Público, 2012); F = Article 17, Section 2 LFPIORPI (Congreso de la Unión, 2012); G = Article 18, Section 1 LFPIORPI (Congreso de la Unión, 2012); H = Article 18, Section 2 LFPIORPI (Congreso de la Unión, 2012); I = Article 18, Section 4 LFPIORPI (Congreso de la Unión, 2012); J = Article 19 of LFPIORPI (Congreso de la

Unión, 2012); K = Article 32 LFPIORPI (Congreso de la Unión, 2012); L = Article 20 RLF (Secretaría de Hacienda y Crédito Público, 2013a); M = Article 22, Section 2 RLF (Secretaría de Hacienda y Crédito Público, 2013a); N = Article 34 RCG (Secretaría de Hacienda y Crédito Público, 2013b); O = N/A – Mobile Payments Must be Linked to Bank Account (Suárez, 2016); and, P = SHCP Advisory, Sept., 2015 (Secretaría de Hacienda y Crédito Público, 2015)

Appendix D – Mexico: National Money Laundering Case Related Statistics

Statistic	2006	2007	2008	2009	2010	2011	2012	2013
MXN Seized (in millions)	N/A	N/A	N/A	247.34	67.82	179.97	354.21	820.41
USD Seized (in millions)	N/A	N/A	N/A	1.19	0.52	0.37	0.04	8.45
Prosecutions	36	45	61	45	70	108	128	84
Convictions	21	18	29	21	27	33	8	15
Acquittals	6	8	8	4	5	5	4	5
Requests for Prosecution (by FIU)	N/A	N/A	38	43	52	39	35	81
Intelligence Reports (from FIU)	N/A	N/A	116	207	70	88	56	0

Note: Money Laundering Case Related Statistics for Mexico. Adapted from *Mutual Evaluation of Mexico: 7th Follow-Up* Report (pp. 9-12) by Financial Action Task Force, 2014, Paris. Retrieved from http://www.fatf-gafi.org/media/fatf/documents/reports/mer/Follow-up-report-Mexico-2014.pdf