

FATF



預付卡、行動支付
與網路付款服務
風險基礎方法指引

2013年6月

FATF 是一個獨立的政府間組織，旨在發展與提升政策，保護全球性金融系統，以對抗洗錢、資恐以及資助武擴。FATF 建議已被認定為全球性防制洗錢與打擊資恐標準。

如需有關 FATF 更完整的資訊，請參閱其網站：

www.fatf-gafi.org

© 2013 FATF/OECD 版權所有。

未取得事前書面許可，不得重製或翻譯本出版品。

本出版品業經 FATF 秘書處授權，由中華臺北行政院洗錢防制辦公室譯為中文，如有出入以公布於 FATF 官網：www.fatf-gafi.org 之英文版為準。

行政院洗錢防制辦公室 2017 年 10 月印製。

目 錄

縮寫對照表.....	1
I. 前言.....	3
A. 範圍與適用對象.....	3
B. 指引之目的.....	6
II. 參與提供 NPPS 之實體所扮演的角色.....	7
A. 預付卡.....	7
B. 行動支付.....	10
C. 網路付款服務.....	15
III. FATF 建議規範之實體.....	18
A. FATF 之「金融機構」定義.....	18
B. 可能豁免 AML/CFT 措施之 RBA.....	20
IV. 風險評估與 NPPS 降低風險.....	21
A. 風險因子.....	22
B. 降低風險措施.....	32
V. 法規對 NPPS 市場的影響.....	40
A. FATF 之普惠金融指引.....	41
B. G20 創新普惠金融原則.....	41
VI. 法規、監管與 RBA.....	42
A. AML/CFT RBA 措施與監督.....	42
B. CDD.....	44
C. 核准/登記.....	48

D.	電匯	49
E.	監管方法以及辨識有權管轄區域	50
VII.	可處理風險的適當 AML/CFT 法規	52
A.	與風險水準呈比例之 AML/CFT 措施	53
B.	決定哪些 NPPS 廠商應遵守 AML/CFT 義務時 應考量的問題	54
	附錄 1-NPPS 之監管方法	59
	參考書目	70

縮寫對照表

AML/CFT	Anti-money laundering/countering the financing of terrorism 防制洗錢及打擊資恐
ATM	Automated teller machine 提款機
CDD	Customer due diligence 客戶審查
G2P	Government-to-person 政府-個人支付系統
IP	Internet protocol 網際網路通訊協定
KYC	Know your customer 認識您的客戶
ML	Money laundering 洗錢
MNO	Mobile network operators 行動虛擬網路業者
MVTS	Money or value transfer services 金錢或價值移轉服務
NFC	Near field communication 近距離無線通訊
NPM	New payment methods 新型態支付工具
NPPS	New payment products and services 新型態支付產品及服務
P2B	Person-to-business 個人-企業支付系統

P2P	Person-to-person 個人間支付系統
POS	Point of sale 銷售點管理系統
RBA	Risk-based approach 風險基礎方法
SIM	Subscriber identity module 用戶辨識模組
TF	Terrorist financing 資助恐怖分子
USSD	Unstructured supplementary service data 非結構化補充服務資料

預付卡、行動支付與網路付款服務之風險基礎方法指引

I. 前言

1. 全球新型態支付產品與服務（NPPS）的快速發展、功能增加以及使用率提高，對各國與私部門在確認該等產品與服務是否遭洗錢（ML）與資助恐怖分子（TF）目的濫用方面帶來挑戰。防制洗錢及打擊資恐（AML/CFT）權責機關在制訂與執行 NPPS 之 AML/CFT 法規時也注意到這點。防制洗錢金融行動工作組織（FATF）2006、2008 及 2010 發佈了新型態支付工具（NPM）態樣報告（typologies report）¹，內容強調：NPM 遭罪犯濫用的可能性；找出可能使一項新型態支付產品或服務在功能上與其他產品或服務產生區隔的風險因子，以及可針對特定新型態支付產品或服務量身規劃以處理特定風險概況之風險減緩策略。任何此一領域新興技術的創新用途，包括分散式數位貨幣。FATF 之討論內容反映了這些疑慮，且將繼續考量必要的風險與措施，藉此減輕其 ML/TF 風險。

A. 範圍與適用對象

2. 本文件提議符合 FATF 建議之 AML/CFT 措施及預付卡、行動支付以及網路付款服務 NPPS 相關法規之風險基礎方

¹ 請參閱 FATF（2006）、FATF（2008）及 FATF（2010）。

法指引。指引不具拘束力，且並未逾越全國權責機關之權限。其目的在依據 FATF 態樣報告及輔助既有 FATF 指引制訂與執行一 AML/CFT RBA，尤其包括 FATF 洗錢/資助恐怖分子風險評估指引（FATF Guidance on ML/TF risk assessment）²；NPPS 亦在普惠金融（financial inclusion）方面扮演了重要的角色。本指引符合「FATF 防制洗錢、資助恐怖分子措施暨普惠金融指引（FATF Guidance on anti-money laundering and terrorist financing measures and financial inclusion）」之規定，前述指引協助各國與金融機構設計符合普惠金融目標的 AML/CFT 措施，而不會影響為打擊犯罪而制訂之既有措施³。就此方面，FATF 瞭解，運用過度謹慎的方式預防 AML/CFT，可能導致將合法業務以及客戶排除在金融系統之外的非預計結果，並因此迫使客戶採用不受法規與監理機關監督的服務。AML/CFT 控管不應限制遭排除在金融服務以外者或遭限制不得與從事銀行活動之人，使用一般金融服務。FATF 瞭解，將相關人士排除在金融服務以外，可能影響 AML/CFT 與普惠金融的有效性，且應將 AML/CFT 視為輔助之用。

3. 於本指引中，NPPS 被視為新穎且創意的支付產品與服務，

² 請參閱 FATF (2013a)。本文件列示可作為評估全國 ML/TF 風險之有用架構的一般原則。然而，這些原則在執行更明確範圍的風險評估作業時，也可能具相關性。本指引的目的亦不在說明監理機關應如何評估風險基礎監督作業之風險。

³ 請參閱 FATF (2013b)。

可作為傳統金融服務的替代方案。NPPS 包括許多牽涉新支付方式或延伸傳統零售電子支付系統的產品與服務，以及未採用傳統系統於個人或組織間移轉價值之產品。在此等產品與服務快速發展與不斷變動的本質下，任何試圖更精確定義 NPPS 意義的作為，皆可能非蓄意的限制本指引文件之適用性。就此方面，很重要是須瞭解，雖然本指引是針對既有 NPPS 而編製，不過可能亦適用本文件未納入考量的新式且新興的 NPPA。為確保本文件所列指引具攸關性且實用，我們尤其將重點放在下列三大 NPPS 類別：(1) 預付卡；(2) 行動支付服務；及(3) 網路付款服務。很重要需注意的一點是，NPPS 間的關聯性越來越高，無論是這三大類別之間或與傳統支付方式間皆同。

4. 傳統金融服務，例如銀行業務服務，有越來越多情況是透過新且創新的方法提供，包括使用網際網路或行動電話技術。然而，雖然各國與金融機構應找出及評估與此等傳統金融服務新交付方法有關的 ML/TF 風險⁴，不過這些並不在本指引的規範範圍內。本指引文件的重點是在創新支付方式以及減輕 ML/TF 風險之措施。
5. 本指引主要規範牽涉 NPPS 法規之公家機關（尤其是監理機關與政策制訂者），以及產業中與設計、開發及提供 NPPS 有關的機構，包括發佈與管理 NPPS 之金融機構，且其中已有許多規範有 CDD 與其他控管措施，以減輕 ML 與

⁴ 請參閱建議 15。

TF 的風險。

B. 指引之目的

6. 本指引之目的為：

- (a) 說明新型態支付系統的運作方式、實體中提供 NPPS 之人，以及其扮演的角色／活動（第 II 部分）；
- (b) 檢視哪些參與提供 NPPS 的實體已經在 FATF 建議適用範圍內（亦即：其屬 FATF 定義之金融機構）（第 III 部分）；
- (c) 判定與提供 NPPS 有關的風險，包括透過考量任何相關風險因子以及降低風險措施（第 IV 部分）；
- (d) 考量法規對 NPPS 市場的影響，包括此等法規是否將影響普惠金融與對現金存款轉移至受規範金融機構的正面意涵（第 V 部分）；
- (e) 檢視如何規範與監督及提供 NPPS 有關之實體、考量該等法規之影響，以及監督執行 AML／CFT 措施（第 VI 部分）；以及
- (f) 依據下列第 III、IV、V 及 VI 部分所述考量因素，討論決定適用 NPPS 可處理風險之適當 AML／CFT 法規時應考量之因素，以及確認可能有多個受規範之實體（第 VII 部分）。

II. 參與提供 NPPS 之實體所扮演的角色

7. 本節說明新型態支付系統的運作方式、實體中提供 NPPS 之人，以及其扮演的角色／活動。NPPS 之架構、特質與營運模式差異甚大，且許多都與處理 ML/TF 風險有關。

A. 預付卡

8. 預付卡是在 1990 年代推出到支付市場中，作為信用卡（需發卡機構評估持卡人最低信用評等）與扣款卡（需於一銀行或金融機構開設有付款帳戶）以外的選項。預付卡原是作為支付商品與服務的裝置，且發卡機構不需針對持卡人的信用評等進行評估，或負擔開設與管理支付帳戶的成本。目前許多預付卡可能備用在提款機（ATM）提領現金，包括跨國提領。此外，部分預付卡還提供個人間支付系統轉帳的功能。

9. 預付卡市場的動能與不斷演化的性質，對 AML/CFT 法規在確保維持相關與最新方面帶來了特定挑戰。今日，預付卡的功能已經有了極大的改變，因其已自替換商店禮券以及有限制目的封閉式迴路應用程式，（在某些情況下）演化為擁有與支付帳戶有關之支付工具所擁有的所有功能。預付卡功能的一端維持在禮物卡的形式，只能在有限網路中向單一商家購買（通稱為封閉式迴路預付卡）。這些卡片無法存取全球 ATM 網路，且無法向商家取得現金退款（通稱為「現金退款（cash back）」）。考量其低風險特質，封閉式

迴路卡片（尤其是不允許儲值或提款之卡片）仍不在本文件規範範圍內，且本文件所載 AML/CFT 措施與法規指引將不適用該等卡片⁵。預付卡功能的另一端則為支付網路品牌的卡片，允許與參與支付網路的任何商家或服務廠商進行交易（通稱為開放式迴路預付卡）。對大部分開放式預付卡來說，客戶將可使用預付卡取得存放於相關支付帳戶的資金。雖然可能將相關資金資料儲存於卡片上的一張晶片，不過預付卡晶片的使用率已經越來越低。部分預付卡可使用現金與其他電子支付工具作為資金來源，所提供的功能與支付帳戶及相關工具移動資金的功能類似，可透過全球 ATM 提款，且於部分情況下，也允許於使用者之間進行個人間支付系統資金移轉。在前述兩種預付款極端案例中，可能有些產品擁有帳戶的部分功能，不過規範限制的作法（例如：儲值門檻、有限支付能力）則可大幅度降低風險。

10. 許多實體可能參與提供預付卡的服務。實體所扮演的角色，與預付卡產品的營運模式息息相關，且單一實體可能扮演各種角色或透過代理人提供服務，此等情況可能對主管機關在決定應在哪些部分規範適當 AML/CFT 控管措施方面帶來挑戰。本文件在第 VII 部分提供了指引，以協助各國決定在特定預付卡營運模式中，應以哪一實體（或多

⁵ FATF 並不認為封閉式迴路預付卡不存在任何 ML/TF 風險，而是認為 ML/TF 的風險可能（舉例來說）因限制該等卡片的用途而降低。

個實體)擔任負責的一方(或多方),且因此需符合 AML /CFT 法規的規定。參與提供預付卡服務之實體可能包括下列各方:

- (a) 收單機構 (Acquirer) - 係指維持與零售商關係之實體,提供接受卡片付款所需之基礎架構(例如:存取銷售點管理系統(POS)終端機,或支援電子商務網站之支付服務),且通常擁有可存放銷貨收入的帳戶。
- (b) 經銷商(包括零售商) - 係指代表發卡機構銷售、提供或安排銷售預付卡給消費者的實體,經銷商亦可能為客戶提供多種服務。
- (c) 支付網路營運商(Payments network operator) - 係指提供技術平台以於 ATM 或商家銷售點進行交易之實體。
- (d) 發卡機構 - 係指發行預付卡,且客戶可向其贖回或提領資金之實體。
- (e) 計畫管理公司(Programme manager) - 係指負責制訂並與銀行或電子貨幣機構合作管理預付卡計畫之實體。計畫管理公司通常會行銷預付卡以及與銀行及經銷商或客戶建立關係,且在許多案例中,還會提供資料處理服務。部分預付卡發卡機構也會自行管理其卡片計畫(亦即:未採用計畫管理公司)。
- (f) 代理商 - 於本指引中,代理商係指代替參與提供預付卡服務之其他實體提供預付卡服務的任何自然人或法

人，無論係因與該等個體簽約或依據該等實體指示而執行皆同。參與預付卡市場的實體，可能會經常代表其他實體，視預付卡計畫所選擇的營運模式而有所不同。

B. 行動支付

11. 今日的行動支付服務是在行動電話於 1990 年代末期間世後不斷演化後的產品，此等演化過程的第一階段，與行動電話既有的資料通訊能力有關，銀行注意到行動電話的這個特質，並且開始提供基本的查詢服務，例如帳戶餘額查詢，並逐漸開始擴展功能範疇至包括交易服務，例如資金移轉。此等服務一開始合稱為「行動銀行」，在此階段，銀行的大部分功能是擔任提供行動支付服務的廠商。如上所述，「行動銀行」及透過其他創新通路提供的傳統金融服務，仍然不在本文件規範的範圍內。此等行動銀行服務與以銀行為主體的行動支付模式非常不同，後者用於提供新產品或服務給新客戶，詳細說明如下。
12. 第二個階段與行動電話通訊進一步擴展以及在電子貨幣產品方面的經驗有關，各種實體在此等環境下，嘗試針對「透過行動電話進行交易」的主要設計概念執行電子貨幣產品交易，以及透過經營預付模式之零售商經銷網路進行交易。在此階段中，在行動貨幣產品通常與預付帳戶連結的前提下，非金融業實體的表現也十分活躍。事實上，電

信廠商就是非常成功的行動貨幣發行機構。於此階段中，有幾個管轄區域已經出現前述發展，並且不是允許這樣的模式在無特定法規的情況下發展，就是以特許、需進行註冊或禁止營運的方式進行規範。然而，在新興市場中，行動貨幣的形式（包括行動支付）正在不斷成長，並為普惠金融做出了貢獻，因為此模式讓無法取得足夠服務以及無法進行銀行業務的消費者，能夠運用多種形式的正式金融服務。

13. 今日，協助提供行動支付服務（包括個人-企業支付系統（P2B）、個人間支付系統（P2P）或政府-個人支付系統（G2P）交易）的金融機構，可以是傳統支付服務廠商（銀行或存款機構）或非銀行支付服務廠商，於 FATF 詞彙表則稱為「金錢或價值移轉服務（MVTs）」。依據營運模式以及所採用技術的不同，各種服務廠商成為了金融機構提供行動支付服務的必要合作夥伴。這些合作夥伴包括行動虛擬網路業者（MNO），且可能包括行動電話設備製造廠商、電信產業標準制訂群組、支付網路以及軟體開發商。就所使用技術方面，各營運模式採用各種方法協助行動支付，包括文字簡訊、行動網路存取、近距離無線通訊（NFC）、用戶辨識模組（SIM）卡以及非結構化補充服務資料（USSD）。
14. 各營運模式間之行動支付服務的性質與營運差異甚大，且通常包括新技術以及與其他種類 NPPS 間的連結，因此對

各國在開發有效 AML/CFT 法規方面帶來了挑戰。營運模式因主導服務廠商以及所採用技術平台之不同而可能會有很大差異，無論服務費用預付或後付（亦即客戶於收到服務後才付款）皆同。下列行動支付服務模式的說明並非無所不包，且並非說明任何特定計畫，而是提供行動支付服務典型特色的一般敘述，以協助開發與應用 AML/CFT 措施與法規。

15. 於以銀行為主體的行動支付模式中，客戶為提供行動支付服務之銀行的帳戶持有人。然而，這與透過行動電話提供傳統銀行業務服務並不相同，因為銀行可能開發透過行動電話提供之新產品，以對過去未有銀行業務往來，而僅擁有有限功能交易帳戶的客戶提供服務；銀行亦可能擔任與支付帳戶無關的電子貨幣提供廠商。銀行與軟體開發商及付款處理廠商（payment processor）合作，讓銀行客戶能夠透過行動電話存取機制寄送與收取付款訊息，款項則透過本國自動清算網路或支付卡網路結算，資金將會自客戶銀行帳戶或支付卡帳戶提領及／或存入該等帳戶。MNO 在此範例中所扮演的角色僅限於提供電信網路設施傳送付款訊息，且並未於任何階段管理或保管客戶的資金。因此，MNO 將不需取得任何金融服務執照，因銀行為支付服務廠商。
16. 在以 MNO 為主體的行動支付模式下，MNO 提供行動支付服務，作為增加其通訊服務價值的一個方法。通常客戶資

金會保管在由 MNO 本身或其子公司所管理的預付帳戶中，雖然在某些管轄區域，即使 MNO 是業務負責人（business owner）（承擔提供服務之全部財務風險以及營運責任的實體），不過通常是合作夥伴銀行擁有正式執照。若資金係後付，則 MNO 可視為提供短期授信或支付服務予客戶，方式同部分三方支付卡計畫。⁶ 就此方面，預付帳戶消除了 MNO 的授信風險，而擁有後付帳戶的客戶，則與 MNO 建立授信關係。MNO 通常為有能力提供跨國服務之跨國公司，此等情況亦適用無提供跨境支付服務之法律面或技術性障礙的支付服務。

17. 於上述兩個例子中，合作創造代理網路為各地理區域新客戶提供服務的金融機構與 MNO，可提供各種行動支付服務，而在銀行業務系統下，這些地區往往無法獲得足夠的服務。於此等情況下，MNO 零售銷售通路及其他店面零售商，將為該等有限目的銀行分行提供類似服務，包括與客戶簽署契約、接受存款以及支付現金以結清行動支付交易。支付服務可能以銀行名稱或 MNO 名稱提供。
18. 行動支付服務與其他支付服務間的互動越來越多。MNO 與 EFT 網路合作，讓國內客戶能夠在輸入密碼之後，自 ATM

⁶ 於本模式中，發行機構（與持卡人有往來關係）及收單機構（與商家有往來關係）為同一實體，這代表發卡機構與收單機構間不需收取任何手續費。本模式為特許經銷商之模式，每個市場只會有一特許經銷商，且此亦為本模式之誘因。因此相同品牌內不會有競爭活動存在，而是與其他品牌競爭。

提領現金，而非使用支付卡。為讓客戶能夠跨國提領現金，MNO 與支付卡發卡機構合作提供開放式迴路預付卡。

19. 透過行動電話而僅限向單一或有限數量商家購買有限價值產品（例如：應用程式或鈴聲）之行動支付服務，不在本文件規範範圍內。部分以此方式經營的行動支付服務，與封閉式迴路預付卡類似，且本文件所規範之 AML/CFT 措施與法規指引並不適用該等服務。茲此釐清，本指引之用意並非處理由 MNO 建立、銷售、移轉或耗用預付或後付客戶「通話時間」餘額之作業。然而，本指引可能適用「通話時間」資金可移轉及接受為付款或替代貨幣之情況。
20. 許多實體可能參與提供行動支付服務。此等實體所扮演角色依據行動支付服務營運模式之不同而有所差異，且各種角色可能有單一實體扮演或透過代理商扮演。⁷ 這可能為法規帶來如何決定誰應負責 AML/CFT 控管作業的挑戰。本文件於第 VII 節中，提供適用各國的指引，瞭解哪一個（或多個）實體在特定行動支付營運模式中可能被視為應負責之一方（或多方），且因此需遵守 AML/CFT 法規之規定。參與提供行動支付之實體可能包括下列：
 - (a) MNO – 係指提供技術平台以允許透過其行動電話存取資金之實體。

⁷ 參與行動支付市場的實體，依據行動支付服務所選定營運模式的不同，經常會擔任其他實體的代理人。

- (b) 經銷商（包括零售商）– 係指銷售或安排代表發卡機構發出資金予消費者的實體，前提是該等資金可用於支付款項。經銷商可能向其客戶提供各種服務，例如技術支援。
- (c) 電子貨幣發卡機構 – 係指發行電子貨幣之實體。於本文件中，電子貨幣是消費者可使用、儲存於一支付裝置上的資金或價值紀錄，例如預付卡、行動電話或電腦系統上之晶片，作為銀行或非銀行實體所屬非傳統帳戶⁸之用⁹。

C. 網路付款服務

- 21. 網際網路開啟了電子商務的世界，並且導致各種網路付款服務於 1990 年代後期開始發展，作為線上買家與賣家（P2B）以及個人移轉（P2P）交易的中介機構。於過去十年期間內，金融機構與零售商持續開發出各種使用網際網路的電子支付工具，並提供給各領域消費者使用。¹⁰
- 22. 網路付款服務提供各項機制，讓客戶能夠透過網際網路、預付帳戶存取，並用於將該等帳戶中所持有的電子貨幣或

⁸ 於本定義中使用「帳戶（account）」，並未預先判定各國所提出與是否建立業務往來關係有關的問題」（請參註腳 38）。

⁹ 此一電子貨幣定義，係採用世界銀行「全球創新零售支付：概況（Innovations in Retail Payments Worldwide: A Snapshot (July 2012)）」報告之定義。電子貨幣的定義應保持彈性，因其可能需進一步與網路貨幣、M Money、電子皮包以及電子錢包做出區隔。

¹⁰ 請參閱世界銀行報告（2012）。

價值移轉予於相同服務廠商開設有帳戶的其他個人或公司。受款人接著會以支付或提領資金的方式，向發卡機構贖回移轉的價值。提領作業可能透過移轉資金至一般銀行帳戶、預付卡或其他 MVTS 進行。雖然客戶通常會在預付帳戶存放一些資金，不過客戶並不需存放。當帳戶需要資金使用時，可透過自銀行帳戶或支付卡帳戶扣款，或於必要時透過其他資金來源供應。

23. 許多網路付款服務採用多種營運模式，此等服務被稱為數位錢包、數位貨幣、虛擬貨幣或電子貨幣。網路支付服務的功能、架構與程序差異可能非常大。相關服務可能允許個人轉帳給申購服務的任何個人或公司，或可能限制只能向特定商家或線上環境進行交易。網路付款服務亦可能與其他支付方法產生關聯，例如預付卡。
24. 數位貨幣廠商可能允許第三方從事以國幣交換電子貨幣或價值的交易。於此等營運模式之下，電子貨幣可能透過該等代理商發行與贖回。這些代理商可能與相關廠商有（或無）聯屬關係，且因此擔任虛擬貨幣交換機構。採用此一模式經營的廠商，係透過帳戶對帳戶移轉的方式賺取收入。交換機構銷售其帳戶中的數位貨幣、移轉其帳戶中的價值至客戶的帳戶。當付款收受方希望換取現金時，前述流程即反轉操作。透過購買或銷售數位貨幣換取現金（或其他數位貨幣），交換機構將擔任虛擬貨幣交換機構的角色。

25. 另一個常見的網路付款服務形式，是線上銷售貴金屬數位表彰權利之數位貨幣廠商。此等服務廠商依據市價銷售虛擬黃金或白銀，宣稱代表客戶擁有實際貴金屬。中介機構（或通稱交換機構），以其帳戶與客戶進行數位貴金屬購買與銷售交易。此等交換機構將自行決定用來交換數位貨幣的支付形式。
26. 消費者用於支付線上投標款的預付帳戶，為最主要的網路付款服務。收受方可能需（亦可能不需）向支付服務廠商註冊，收取資金移轉款項。客戶可能使用一般銀行帳戶，將款項預付至網路支付帳戶。網路付款帳戶中之資金可用於移轉給同一廠商的其他客戶，或轉回客戶的一般銀行帳戶。
27. 網路付款服務亦可能與線上博奕或虛擬世界有關，該等交易僅能使用專屬形式的貨幣進行。交易參與人於帳戶中持有代幣，並使用該等代表作為與封閉線上環境中的其他參與人或零售商交易的資金。專屬貨幣的收受方，可於退出該環境時換取其所在國貨幣。
28. 與僅為向電子貨幣發卡機構購買產品或服務之目的，或為向有限商家購買有限價值產品與服務之目的，而發行電子貨幣之網路付款服務，不在本文件規範範圍內，因其與封閉式迴路預付卡類似。如同前面所述，本文件所規範之 AML/CFT 措施與法規指引並不適用該等服務。
29. 發展替代性線上貨幣仍為 AML/CFT 政策制訂者及私人機

構的主要考量重點。雖然某些貨幣可能落在本指引文件範圍之外，許多指引的許多要件也可能適用。政策制訂者應瞭解此等既有或新興電子產品、服務與貨幣形式，並監督其市場之發展，以瞭解相關潛在風險及開發適合之政策。考量線上貨幣不斷發展之特性，FATF 可能考慮在未來進一步研究此一領域之規定。

30. 如上所述，網路付款服務可由金融機構或非金融機構提供。本文件於第 VII 節中提供各國指引，瞭解網路付款服務中哪一實體（或多個實體）應視為負責廠商，因此需遵守 AML/CFT 法規。

III FATF 建議規範之實體

31. 本節檢視哪些參與提供 NPPS 的實體已經在 FATF 建議適用範圍內（亦即：其屬 FATF 定義之金融機構）。
32. 依據 FATF 建議，各國應確保金融產業與其他指定產業適用預防性措施。雖然 NPPS 廠商提供了落在 FATF 建議範圍內的產品與服務，不過有時因為參與實體的範圍以及 NPPS 的複雜度，很難決定哪一實體應該負責執行 AML/CFT 預防性措施。因此，本文件為各國提供將 FATF 建議適用至 NPPS 廠商之指引。

A. FATF 之「金融機構」定義

33. 將 AML/CFT 預防性措施適用到 NPPS 時，各國應考量哪

一實體落在 FATF 建議範圍內。於決定金融機構時，FATF 在詞彙表中提供了一份應適用 AML/CFT 之金融活動或營運的清單。

方塊 1：FATF「金融機構」定義

金融機構係指以公司型態代表客戶從事下列活動或營運之任何自然人或法人：

1. 接受大眾存款及其他可返還資金¹¹
2. 放款¹²
3. 財務租賃¹³
4. MVTs
5. 發行及管理支付方法（例如：信用卡與扣款卡、旅行支票、匯票及銀行本票、電子貨幣）
6. 財務擔保與承諾
7. 買賣：
 - (a) 貨幣市場工具（支票、票據、存款憑證、衍生性商品等）；
 - (b) 外匯；
 - (c) 交換、利率與指數工具；
 - (d) 可轉讓證券；

¹¹ 此亦包括私人銀行。

¹² 尤其包括：消費者授信、抵押借款授信、應收帳款融資（無論是否有追索權）以及商業交易融資（包括沒收）。

¹³ 此點未延伸適用與消費性產品有關的財務融資安排。

(e) 商品期貨交易。

8. 參與證券發行及提供與此等發行有關之金融服務
9. 個別與集合投資組合管理
10. 代表他人保存與管理現金或流動性證券
11. 以其他方式代表投資、處理或管理資金或貨幣
12. 承保與募集人壽保險與其他投資相關保險¹⁴
13. 貨幣與貨幣兌換

34. NPPS 廠商因從事 MVTS，或發行與管理支付方法而落在金融機構定義之範圍內，且因此應依據 FATF 建議規定遵守 AML/CFT 預防性措施規定，包括（舉例來說）：CDD、記錄保存與通報可疑交易。然而，在決定提供 NPPS 中哪一（或多個）實體應負責執行預防性措施以及於全國層級適用此等措施方面可能會有所困難。本文件於第 VII 節提供各國指引，俾瞭解哪一個（或多個）實體應視為負責之 NPPS 廠商，並因此需遵守 AML/CFT 法規。

B. 可能豁免 AML/CFT 措施之 RBA

35. 於特定情況下，各國可能豁免金融機構定義所列活動適用 FATF 建議之預防性措施。建議 1 之註釋規定，在兩種情況下，各國得決定不適用部分 FATF 建議中規定金融機構應採取之行動：

¹⁴ 此點適用保險事業與保險中介機構（仲介與經紀商）。

- (a) 前提是可證明 ML 與 TF 風險低；此點嚴格適用於有限且有合理佐證之情況，且與特定種類金融機構或活動或 DNFBP 有關；或
 - (b) 若一金融活動（非移轉貨幣或價值）係由一自然人或法人於偶發或非常有限的基礎下（考量其量化與絕對要件）所執行，則前提是 ML 與 TF 風險低。¹⁵
36. 各國應注意，建議 1 之註釋另外規定，若所蒐集之資訊與其風險水準不符，則建議 11 有關保存資訊之規定，應適用於所蒐集到的任何資訊。各國就 NPPS 應注意的其他相關要件是：MVTS 不得因金融活動係偶發或於非常有限情況下執行，而可豁免適用前述規定。¹⁶

IV. 風險評估與 NPPS 降低風險

37. 為執行 AML/CFT RBA 及 NPPS，各國及私部門機構在設計 NPPS 時，必須辨識 NPPS 所存在的 ML/TF 風險。依據 FATF 建議 1 規定，各國應辨識、評估與瞭解該國的 ML/TF 風險¹⁷，且亦應要求金融機構辨識與評估 ML/TF 風險。¹⁸ 特別與 NPPS 有關的是建議 15，要求各國與金融機構辨識及評估因開發新產品與營運實務，以及使用新技術或開發技術有關的 ML/TF 風險。此外。依據建議 15 規

¹⁵ 請參閱建議 1 註釋第 6 條 [FATF (2012)]。

¹⁶ 建議 10 規定，金融機構於執行偶發電匯交易時，需採行 CDD 措施。

¹⁷ 本指南文件所稱一國或各國，同樣適用區域或管轄地。

¹⁸ 請參閱 FATF 建議之建議 1 與建議 1 註釋。

定，各國亦要求金融機構應於開始採用新產品、營運作業實務或使用新技術前，辨識與評估風險。¹⁹

38. 本節說明各種風險因子與降低風險措施，藉以協助各國及私部門機構評估 NPPS 風險。於評估 NPPS 所帶來風險時，各國應將考量 FATF ML/TF 風險評估指引²⁰。此外，各國與金融機構皆應將建議 10 之註釋就 CDD 所列示風險因子納入考量。雖然此等釋例並非 FATF 建議的必要要件，不過這些資料提供了風險指標的有用釋例，其中許多將在以下與 NPPS 所帶來 ML/TF 風險有關之章節中詳細說明。

A. 風險因子

39. 本文件之本節，列示有助於辨識與 NPPS 有關之 ML/TF 風險之風險因子。許多 NPPS 可能存在降低 ML/TF 風險之特質，且此等特質應視為評估特定 NPPS 相關風險之整體方法。特定 NPPS 之 ML/TF 風險程度，將依據所有風險因子、既有風險減輕措施及其功能而判定。

i. 非面對面關係與匿名

40. 與許多銀行業務方法相同，NPPS 可能允許建立非面對面的

¹⁹請參建議 15：「各國與金融機構應辨識與評估因下列情況而可能發生的 ML 與資助恐怖份子風險：(a) 開發新產品與新營運實務，包括新交付機制；及 (b) 為新產品及既有產品使用新技術或開發技術。就金融機構方面，此等風險評估作業應於發表新產品、營運實務或使用新技術或開發新技術前執行，其應採取適當措施管理與降低此等風險」。

²⁰請參 FATF (2013a)。

業務往來關係。依據其特質之不同，NPPS 可能用於快速在全球各地透過 ATM 網路搬移資金、進行採購以及取得現金（直接或間接）；缺乏面對面接觸可能代表更高的 ML/TF 風險狀況。若客戶之身分與驗證措施不足以處理與非面對面接觸有關的風險，例如模仿舞弊，則 ML/TF 風險將會提高，而且將難以追蹤資金。

41. 雖然監控與報告機制可用來辨識可疑活動，缺乏 CDD 將會增加服務廠商完成此等作業的困難度。舉例來說，將影響服務廠商發現客戶同時擁有多個帳戶的能力。
42. 就預付卡而言，當客戶購買、登記、儲值、重複儲值或使用卡片時，將會產生因匿名而帶來的風險（無法辨識客戶）。匿名所帶來的風險高低，於卡片所擁有的功能以及是否存在 AML/CFT 降低風險措施有關，例如資金來源或購買上限、儲值上限、取得現金，以及卡片是否能夠在發行國以外使用。預付卡可以經由不同 CDD 程度的各種方法儲值，包括透過銀行、網際網路、小型零售商店或 ATM。雖然透過銀行帳戶或網際網路儲值通常源自於可辨識持卡人的帳戶或支付工具，不過也可能透過其他 NPPS 提供現金或資金，而且可能也完全匿名。此外，預付卡也可輕易的交由發卡機構所不知悉的第三方使用，包括但不限於特別為允許第三方匯款之「雙卡（twin cards）」設計，以及以可匿名作為產品特點進行廣告。若這些產品的廠商位於各預付卡廠商未受 AML/CFT 足夠規範與監督的國家，且於世

界各國銷售其產品，則這可能是需要注意的一點。²¹

43. 行動支付服務可能透過代理商、線上或行動支付系統建立客戶往來關係，同樣的通路將被用於儲值資金至行動帳戶。當行動支付服務被使用或重複儲值時，將會產生匿名風險，且此點與行動支付服務之功能，以及是否規範有 AML/CFT 降低風險措施息息相關，例如 CDD 或資金使用門檻。
44. 就網路付款服務而言，通常不會有面對面的客戶接觸，而在未執行處理相關風險有效措施的前提下，這將增加身分冒用或客戶提供不正確資訊以掩飾非法活動的風險。然而，缺乏面對面接觸的風險，通常可透過採用替代身分驗證機制加以克服，而這可提供足夠的降低風險措施。於使用或重複儲值網路付款服務時，因匿名或未辨識客戶所帶來的風險高低，則與服務之功能、資金來源機制（若資金來自受規範之帳戶，則風險可大幅度降低）以及是否存在 AML/CFT 措施有關。

ii. 地理區域規定

45. 特定 NPPS 可用於全球支付款項與移轉資金之範圍，在決定風險高低時，是一個應納入考量的重要因子。
46. 開放式迴路預付卡，通常允許客戶透過全球支付網路於國

²¹ 此實務規範於 FATF (2010) 第 3 章：「NPM 風險評估 (Risk Assessment of NPM)」。

內與外國銷售點支付生效，此等卡片可於接受任何類似品牌卡片（扣款卡或信用卡）的任何地方作為支付方法。預付卡廠商可能位於一個國家，然後透過代理商或網際網路在全球銷售產品。此等卡片接著可被用於全球購買產品與服務或提領現金。此外，某些預付卡計畫允許持卡人自個人間支付系統移轉資金。某些預付卡能夠在全球支付款項、提領現金以及移轉資金的特性，使該等成為 ML/TF 的理想標的。預付卡的體積很小，亦使其潛在容易成為罪犯用於實體跨境運輸價值工具，而非使用現金。可用於全球提領資金的預付卡，因為具有不會引人注目、帳戶中存放高資金價值且無法從卡片外觀判斷的物流優點，使其特別容易成為遭罪犯濫用的目標，而非透過現金運送業者運送金額龐大、數量眾多的現金。各國亦應考慮建議 32 規定是否適用特定預付產品，例如預付卡，而需歸類為無記名可轉讓金融工具。

47. 可用於全球移轉資金或可用於廣泛地理區域、擁有大量交易相對方的行動支付服務及網路付款服務，較純粹本國營運模式而言，更容易成為罪犯 ML/TF 之目標。此外，位於一管轄區域的 NPPS 廠商，可能提供此等服務給位於其他管轄區域且需受不同 AML/CFT 義務規範與監督的客戶。若 NPPS 廠商位於 AML/CFT 控管薄弱的管轄區域，則應將前述因子納入考量。

iii. 提供資金的方法

48. NPPS 取得資金的方法，將會影響其所具有的 ML/TF 風險高低。匿名提供資金的方法，隱匿了資金的原始來源，創造了較高的 ML/TF 風險。現金具有最高的潛在風險，因現金不具名且無任何交易紀錄。然而，雖然 NPPS 提供了交易監控的平台，NPPS 產品透過其他支付服務取得無法驗證客戶身分之資金的情況，亦可能創造匿名資金提供機制。此外，使用預付模式且不對廠商造成授信風險的 NPPS，可能降低廠商執行完整 CDD 的誘因，因此增加了 ML/TF 風險。
49. 預付卡所帶來的 ML/TF 風險，將因允許以現金提供資金而增加，且某些少見案例中，甚至未對卡片帳戶或 CDD 規定加諸任何儲值上限規定。如此將使預付卡容易遭罪犯濫用，舉例來說，透過將犯罪所額投入金融系統，或使用預付卡作為實體跨境運輸現金的替代工具。
50. 行動支付服務允許帳戶與交易透過不同方法取得資金，許多服務（無論是以銀行為主體或以 MNO 為主體的模式）都會從銀行或支付卡帳戶中提取資金，其他則允許透過代理商網路提供現金資金。雖然前述資金提供方法限制了 ML/TF 風險（不過也限制潛在取得資金的能力），現金與非銀行支付方案開啟了使用支付系統的機會，卻也隱藏了資金來源，並因此提高 ML/TF 的風險。提供帳戶對帳戶轉移功能的行動支付服務，也允許透過第三方提供資金，因

此若未適當辨識資金提供帳戶的所有人，則可能增加 ML/TF 風險。

51. 允許第三方以匿名方式提供資金的網路付款服務，可能面臨較高的 ML/TF 風險。一個由第三方提供資金的特別案例，是使用交換機構或虛擬交換機構。若此等交換機構於轉售已發行之數位貨幣或電子貨幣資金時，接受（其他網路付款服務廠商）遭限制的支付方法，則該機構將可規避網路付款服務廠商對特定資金提供方法的限制（例如：「不接受現金」政策）。此外，廠商將僅在監控時看到交換機構的名稱，不過將不會看到實際指示交換機構將資金匯入帳戶之人。

iv. *提領現金*

52. 透過國際 ATM 網路提領現金，增加了 ML/TF 的風險。此等提領現金的行為，（如預付卡的情況）可能使資金在一個國家提供，而提款行為則在另一個國家進行。相反的，行動支付服務與網路支付服務則與其他 NPPS 間的關係越來越密切，例如間接允許提領現金之預付卡。

v. *服務的區隔*

53. 提供 NPPS 通常包括牽涉數個交易方執行支付交易的複雜基礎架構。預付卡可能牽涉數個交易方執行交易，包括計畫管理公司、發卡機構、收單機構、支付網路、經銷商與

代理商，而行動支付服務廠商通常需協調數家相關服務廠商，並與國際交易相對方合作提供跨境交易。

54. 大量交易相對方參與提供 NPPS（尤其牽涉數個國家）時，因潛在切割困難與潛在遺失客戶與交易資訊等原因，而將增加產品的 ML/TF 風險。若未清楚辨認哪個參與實體需遵守 AML/CFT 義務、誰應負責遵守該等義務，以及哪個參與交易流程的國家需負責規範與監督遵守 AML/CFT 措施的責任時，則將會是一個需要特別考量納入的問題。
55. 採用代理商以及依賴非聯屬第三方辨識客戶關係以及再次儲值，將增加潛在 ML/TF 風險，尤其所蒐集的資訊未與負責遵守 AML/CFT 規定的實體分享時更是如此。負責客戶往來關係所有層面的服務廠商（亦即：註冊、現金匯入/現金匯出與交易），其風險則可能較低，其中較有關係的是訓練、管理與控管流程代理商網路的組織架構以及設定。
56. 此外，提供 NPPS 的實體，通常來自不熟悉 AML/CFT 控管的產業，例如 MNO。因此，CDD 專業知識可能限於（舉例來說）與傳統銀行業比較，且 CDD 通常會被限制在分析特定交易以及經銷商的回饋。此外，資訊鏈也可能為追查資金帶來困難。舉例來說，單一金融交易的資訊鏈可能包括較多實體，其中有部分位於其他國家，而這可能減緩調查程序，而且將進一步因為貨幣流入的速度，以及在試圖扣押與凍結可透過 NPPS 快速移轉或轉運至其他國家

的犯罪所得時所面臨的挑戰而變得更為複雜。

57. NPPS 廠商維持銀行帳戶及使用銀行業務系統執行定期交易，以與代理商及 MVTS 合作夥伴結清帳戶。然而，雖然結清 NPPS 廠商間批發交易的銀行需就 NPPS 廠商負擔 CDD 義務，不過這點並無法瞭解或僅能有限瞭解 NPPS 廠商之客戶，且無法監控 NPPS 廠商與其客戶間的交易。
58. 需遵守 AML/CFT 規定、負責客戶往來關係所有層面的網路付款服務廠商（亦即：註冊、現金匯入／現金匯出與交易），其風險可能低於分散服務廠商。倚賴非關係第三方發行或贖回電子貨幣的廠商，亦可能導致服務遭切割而增加 ML/TF 風險。網路付款服務的切割尤其與其跨境性質有關，亦即廠商可能位於 AML/CFT 法規與監督不足的管轄區域內。

vi. 風險矩陣

59. 下列風險矩陣²²列示一系列有助於辨識與任何種類個別 NPPS 有關的風險因子（雖然並非無所不包），包括預付卡、行動支付及網路付款服務。於評估與特定 NPPS 有關的風險時，很重要的是採取整體評估的作法。我們不應將矩陣表中所列風險因子一一單獨考量，而是應將風險、風

²²此風險矩陣圖是 FATF 在 2010 年發佈的類型報告「運用新支付方法 ML (Money Laundering Using New Payment Methods)」中首次採用，該報告為前一版本 FATF 類型報告「新支付方法報告 (the Report on New Payment Methods (2006))」的更新版本。

險減緩策略以及特定 NPPS 之功能一併考量，以決定產品是否存在高或低 ML/TF 風險。下列風險因子僅供說明之用，且部分 NPPS 可能同時包括應予以考量的較高與較低風險因子，並於與既有風險減緩策略合併後，決定整體風險水準。

60. 雖然風險矩陣完全適用 NPPS，不過若與其他支付工具（例如信用卡與扣款卡）相比較，NPPS 的性質與功能差異可能甚大，且產品可以不同方式為不同使用者量身規劃。基於此一理由，NPPS 風險評估作業應視情況執行，並將單一產品的特定性質納入考量。執行此等作業時，應將與 NPPS 相關的下列特定風險納入考量。

表 1：支付方法風險因子¹

要件		現金 ²	NPM 較高風險因子	NPM 較低風險因子
CDD	辨識	匿名	匿名	已辨識客戶
	驗證	匿名	客戶的身分（取得時）未以可靠、獨立來源文件、資料或資訊進行驗證。	客戶的身分（取得時）經過可靠、獨立來源文件、資料或資訊進行驗證。（Rec.10）
	監督	無	無	持續監督業務往來關係
紀錄保存		紀錄由權責機關透過跨境申報方式產生（R.32）	產生電子交易紀錄，不過未保存，或於執法機關（LEA）提出要求時提供	電子交易紀錄已保存，並於 LEA 提出要求時提供
價值	帳戶 / 每	紀錄由權責	無上限	金額上限

要件		現金 ²	NPM 較高風險因子	NPM 較低風險因子
上限	人帳戶儲值最高限額	機關透過跨境申報方式產生(R.32)		
	每筆交易最高金額（包括儲值／提款交易）	無上限	無上限	金額上限
	最高交易次數	無上限	無上限	交易上限
提供資金方法		不適用	匿名提供資金（例如：現金、匯票、匿名 NPM）；另外還有多種資金來源：例如：第三方	透過於受規範金融或授信機構持有之帳戶，或於其他需遵守適切 AML／CFT 義務與監督之已辨識來源提供資金
地理區域限制		某些貨幣的接受度比其他貨幣更廣泛，貨幣可透過中介機構轉換	跨國境移轉資金或提款	僅於國內移轉資金或提款
使用限制	可轉讓性（商家接受）	一般皆可接受	接受商家／銷售點管理系統（POS）數量多（例如：透過使用 VISA 或 MasterCard 標準）	接受商家／POS 數量少
	效用	p2b、b2b、p2p，不得進行線上使用	p2b、b2b、p2p，可進行線上使用	p2b、b2b，可進行線上使用，惟不適用 p2p

要件		現金 ²	NPM 較高風險因子	NPM 較低風險因子
	提款	不適用	匿名與無限制提款 (例如：透過 ATM 提領現金)	有限提款功能 (例如：僅參考帳戶)； 有限提款金額與次數 (例如：每個會計年度少於特定固定次數)
服務 切割	服務廠商 之互動	不適用	數家獨立服務廠商 執行交易之各個步驟，未受有效監督 與協調	全部交易由服務廠 商執行
	委外	不適用	將數個單一步驟委 外；委外至各國， 未受適當保護；缺 乏監督與清楚釐清 責任	所有流程依據高標 準於內部自行完成

表格附註

1. 風險矩陣摘錄自 2010 NPM 態樣報告並強調風險因子，僅兩個欄位的標題從「低／高風險」修改為「較低／較高風險因子」。此點於 FATF 建議一致，該建議亦提及較低／較高風險情境。
2. 「現金」欄位係用於比較 NPM 與現金之風險因子，現金代表較高的 ML/TF 風險。現金的控管係與跨境運輸現金有關，可能適用建議 32 之現金申報或揭露義務規定。建議 32 於符合無記名可轉讓金融工具資格時，可能適用特定產品。

B. 降低風險措施

61. 特定 NPPS 的整體風險水準，在特定情況下，等於上述各風險因子之累積效果。此外，減輕風險程序應與產品或服務所帶來的風險水準成比例。採用比例性原則，能夠處理

特定 NPPS 所帶來的風險，同時維持便利客戶與易於使用的功能。於經考量此等要素且在全國與相關法規架構下，私部門機構應在專案階段將產品或服務之 ML/TF 風險納入考量，以將相關受影響之因素降至最低的方式進行設計。本文件於本節中提供可能降低風險措施的指引，私部門機構於產品設計階段應予以納入考量。

62. 金融機構應於制訂其 CDD 流程與程序前，辨識、評估與理解其提供之 NPPS 所將帶來的風險。金融機構尤其應在新產品與營運作業實務發表之前，特別針對新產品與營運作業實務所將帶來 ML/TF 風險進行風險評估，包括交付機制，以及使用新技術等。這是本流程中很重要的一個步驟，可讓金融機構依據所辨識之風險水準，建立適當的風險基礎 AML/CFT 措施。

i. CDD

63. CDD 是減輕與 NPPS 相關之 ML/TF 風險的有效措施。於 RBA 下，NPPS 廠商應採取措施辨識與驗證其客戶身分之程度，與產品將具有的風險水準攸關，且符合 FATF 建議及相關國家的法律規定。
64. 若 ML/TF 風險較低時，金融機構可執行簡化 CDD 措施，將較低風險的性質納入考量。簡化 CDD 並不代表完全豁免或可不採取 CDD 措施。對建立業務往來關係的 NPPS 廠商

來說²³，簡化 CDD 措施可能是基本與最少應做到，不過仍然必須與下列第 VI 節所列四項 CDD 要件相符合。依據 RBA 規定，客戶種類與範圍、所需交易資訊以及用於滿足此等最低標準的機制，將會與風險水準息息相關。於較低風險情況下，完成建議 10 的 CDD 客戶辨識、驗證與監督規定後，舉例來說，可採取較不密集與正式的資訊蒐集與監督方法，以及信賴與基本產品預計用途相關之適當假設，或採用較不詳細與次數較少的資訊。FATF 建議，提供可認特定種類客戶、國家或地理區域或產品、服務、交易或交付管道具有潛在較低 ML/TF 風險的範例情況。²⁴ 尤其對 NPPS 來說，一個較低風險的釋例是「提供經適當定義及有限的服務給特定種類客戶的金融產品或服務，以增加提升普惠金融之目的」。

NPPS 廠商亦應將 NPPS 客戶可能遭認定屬較高風險之情況納入考量，並確保其制訂相關程序，以於發現較高 ML/TF 風險情況時，執行強化 CDD 措施。²⁵

65. 很重要且應注意的一點是，FATF 建議允許金融機構於基本上不影響正常營運活動以及於 ML/TF 風險可有效管理的前提下，於建立業務往來關係後（而非於建立業務往來關

²³ FATF 建議未定義本概念，而是交由各國決定是否已建立業務往來關係。

²⁴ 請參閱建議 10 IN 第 17 條。

²⁵ 請參閱建議 10 IN 第 15 條及第 20 條。

係之前或期間執行)，以非面對面方式驗證客戶身分。²⁶

66. NPPS 所擁有的功能越強大，越需要強化 CDD。非面對面驗證客戶身分通常需透過第三方資料庫或其他可靠來源驗證取自客戶之資訊，並潛在追蹤客戶之網際網路通訊協定（IP）位址²⁷，且甚至應搜尋網路資料以驗證資訊，前提是資料蒐集作業符合全國隱私權法律規定。於適當時，可能需採用多種技巧有效驗證客戶身分。發現有較高 ML/TF 風險之情況時，應依據風險高低執行強化 CDD 措施。
67. 無論於任何情況下，交易監督及可疑活動通報皆為必要。然而，在取得可靠客戶資訊可能有所困難的情況下，其重要性甚至更高。在無可靠身分證計畫或擁有替代性可靠辨識形式的國家，則更是需要採取相關措施。
68. 預付卡與行動支付服務通常透過代理商或經銷商的廣泛網絡經銷，且服務廠商可能用於執行面對面交易的 CDD 措施。於此等情況下，經銷商或代理商係代替廠商履行 CDD 義務，且計畫管理公司或發卡機構應將經銷商或代理商納入其 AML/CFT 計畫中，並監督其符合相關 CDD 措施規定之情況。
69. 採用代理商讓各機構有機會於客戶實際到場時執行 CDD。

²⁶ 請參閱建議 10 IN 第 11 條。

²⁷ 當使用者連結網際網路後，網際網路服務廠商會動態分配一個獨特的識別編號（類似電話號碼），使 IP 位址的元件，能夠與地理區位置以及特定時間框架一致，並與個人於帳戶登記程序過程中所提供的實體地址進行比較。註：FATF 建議並未規定應蒐集此等資訊。

使用網際網路時，行動服務廠商將需仰賴非面對面辨識與驗證作業。

70. 網路付款服務廠商通常透過網際網路以及用於儲值資金至網路付款帳戶的相同通路，與其客戶建立往來關係。於此等情況下，網路付款服務廠商將需仰賴非面對面辨識與驗證作業。

ii. 儲值、價值與地理區域限制

71. 對 NPPS 設限，只要能夠與其他 AML/CFT 措施合併執行，則可能是減輕 ML/TF 風險的有效機制，例如帳戶與交易監督，以及申報 STR。設定地理區域或儲值限制，亦可減輕 NPPS 可能遭 ML/TF 濫用之風險。限制 NPPS 產品功能至特定地理區域，或購買特定產品與服務，將減少產品對 ML 人士或恐怖分子資助人的吸引力。然而，很重要的是應瞭解此等限制亦可能限制一般產品的吸引力，而且金融機構與各國都應考量任何限制對合法客戶活動所將帶來的負面影響。此等措施應於 NPPS 設計階段之適當時點予以考量與執行。
72. 考量 ML/TF 風險隨著 NPPS 功能增加而提高，金融機構可考慮為客戶提供個人層級的服務，這部分考量應在 NPPS 設計階段視情況執行。就此部分，金融機構得考量採用不同限制規定，舉例來說，NPPS 門檻限制，以確保產品維持較低風險，並因此適用簡化 CDD。於此等情境下，CDD 與

其他 AML/CFT 措施的範圍應隨著功能增加而增加，且風險也將因此提高。

73. 許多預付卡計畫已規定儲值與期限之限制，確保未使用之預付價值不會帶來不必要的 ML/TF 風險。其他常見措施包括限制透過卡片預付及可提領之金額，以及限制將資金再次儲值至預付卡之功能。儲值與期間限制，以及對支付現金提款之能力所加諸的限制，都可減少預付卡對罪犯所具有的吸引力；門檻是設定單一預付卡於一次或規定期間內可儲值最高上限的有效措施。此等門檻的高低應依據風險敏感度判斷，且將依據是否有其他 AML/CFT 措施存在而定。然而，應適當考量消費者保護因素，以確保客戶於其需要運用資金時能夠提領，並且在客戶被拒絕使用預付卡資金時，考量採取適當追索措施。
74. 此外，部分預付卡計畫允許資金於個人間支付系統移轉的功能，可能帶來濫用 ML/TF 的高風險。尤其規定個人間資金移轉可透過預付卡執行時更是如此，對可能移轉金額規定上限可有效減輕 ML/TF 風險，尤其其可被視為現金時更為有效，這點可透過合併移轉上限與儲值或提款限額強化。於採用 RBA 時，可運用預付卡於個人間移轉之最高金額，依據是否存在其他 AML/CFT 措施而將有所不同，例如地理區域限額。
75. 就行動支付服務方面，可針對行動支付帳戶可持有之最高金額設定上限；對單筆交易允許之最高金額設定上限，包

括現金提款；對每日／每週／每月／每年許可之交易次數或累積金額以及現金提款設定上限；或合併前述所有措施。設定地理區域或購買金額上限，可進一步減輕行動支付服務可能遭 ML／TF 之目的濫用之風險。

76. 網路付款服務通常係以分層架構提供予客戶，且應視情況分別予以考量。部分原為於線上環境進行 P2P 交易而設計的數位貨幣，例如於博奕環境中使用，似乎可因於封閉系統內運作而降低 ML／TF 風險。然而，若數位貨幣可與第三方交易並換取本國貨幣時，則其風險水準將隨時提高。

iii. 資金來源

77. NPPS 廠商於評估 NPPS ML／TF 風險時，應將資金來源納入考量並考量限制產品可接受之資金來源。匿名資金來源，例如現金或甚至其他匿名 NPPS，將提高 ML／TF 風險。NPPS 廠商應整體考量透過此等措施降低 ML／TF 風險，且此等限制應許上述其他限制合併採用。
78. 當個人使用現金為一項或多項設有上限規定的 NPPS 儲值時，若其現金金額超過預先規定的個別帳戶或每日單次或多次交易現金儲值上限時，NPPS 廠商可考慮要求該等個人表明身分。

iv. 紀錄保存、交易監督與通報

79. 交易與 CDD 紀錄對 AML／CFT 措施與支持執法單位調查

來說非常重要。支付或資金移轉之交易紀錄最少應包括列示交易相關各方、牽涉之任何帳戶、交易之性質與日期以及移轉金額之資訊。交易之相對規模不必然等於交易紀錄對執法機關所具有的價值，因此所有交易之紀錄皆應予以保存，無論價值高低。所保存之紀錄應足以透過交易重建而追蹤資金來源。

80. NPPS 之電子交易特性，原則上為有效紀錄保存及監督交易設立良好的基礎。依據建議 11 規定，NPPS 廠商應保存與交易相關之所有紀錄與 CDD 資訊至少 5 年期間，或相關國家法律規定之期間。
81. 行動支付擁有專屬交易的發送方與接受方電話號碼，以及發送方及（可能）收受方 SIM 卡資訊。另外，MNO 亦可能擷取與發送方與收受方於交易時確切地點的相關資訊。依據交易規模與性質之不同，地點資訊可能為交易紀錄的有用資料。雖然 FATF 建議未規定應蒐集此等資訊，不過在蒐集資料之行為符合國家隱私權法規規定之前提下，廠商可將其視為監督客戶活動的有用工具。
82. NPPS 廠商應考慮設置可依據 ML 與 TF 態樣與指標偵測可疑活動的交易監督系統，此等監督系統應將客戶風險、國家或地理區風險、產品服務交易或交付管道風險納入考量。交易監督系統亦可用來辨識某一個人或團體所持有的多個帳戶或產品，例如持有多張預付卡。
83. NPPS 廠商應考慮分析所保存之資訊與紀錄，以決定是否有

異常模式或活動發生。當 NPPS 廠商發現懷疑或有合理由懷疑所運用資金為犯罪活動收入或與 TF 相關的交易時，其應依據 FATF 建議及相關國家法律規定，將懷疑狀況通報金融情報中心。

84. NPPS 廠商應謹慎注意無清楚合法或經濟理由之交易或活動。廠商尤其應考量 NPPS 明顯被用於取代銀行帳戶且無明顯正當目的之情況。舉例來說，明顯以不尋常方式使用之預付卡（例如頻繁執行高額交易），在某些情況下可視為異常交易，因預付卡在許多管轄區域可能無法提供如銀行帳戶所提供的類似保護程度（亦即：存款保險保護）或類似利益（例如：利息）。廠商應考量使用預付卡之理由以及所在區域之相關環境。FATF 態樣報告針對 NPM 規範了協助開發有效交易監督系統的進一步指引，尤其是與辨識可疑交易有關的部分。

V. 法規對 NPPS 市場的影響

85. 制訂 NPPS AML/CFT 法規架構時，各國亦應考量法規對 NPPS 市場的影響。各國尤其應確保 AML/CFT 管制措施符合與 NPPS 相關之 ML/TF 風險，且法規架構並未不當或不必要的對既有產品的運作帶來不利影響，或限制新產品的開發。本節討論法規對 NPPS 市場的影響，包括此等法規是否將影響普惠金融。

A. FATF 之普惠金融指引

86. 2011 年 6 月，於 G-20 要求準則制訂機構協助各國以符合普惠金融規定之方式應用其標準後，FATF 發佈了「FATF 指引：防制 ML 與 TF 措施及普惠金融」。²⁸ 雖然該指引並未特別規範支付方法，不過也將行動支付與預付卡視為有助於普惠金融的支付工具。另外亦需注意的是，部分政府透過採用 NPPS（例如預付卡）支付公共補貼款的方式推廣普惠金融，因該等方法對補貼款受益人而言可能較容易運用。FATF 之普惠金融指引，為各國及其金融機構在設計符合其普惠金融目標，且未影響既有打擊犯罪措施的 AML／CFT 措施時提供了支援。

B. G20 創新普惠金融原則

87. G20 創新普惠金融原則²⁹ 係於 2010 年度發佈，以推廣於制訂法規減輕產品風險時，應採用比例原則，藉以避免加諸可能扼殺創新的不必要法規負擔³⁰。整體而言，比例要件已規範在 FATF 建議中。比例要件允許各國採用 RBA，舉

²⁸ 請參閱 FATF (2013b)。

²⁹ 請參閱創新普惠金融原則與報告 (Principles and Report on Innovative Financial Inclusion (2010))。

³⁰ 請參閱「比例原則第 8 條：基於對現有法規之落差與障礙之理解，建立符合創新產品與服務相關風險與利益之政策及法規架構 (Principle 8 on Proportionality: Build a policy and regulatory framework that is proportionate with the risks and benefits involved in such innovative products and services and is based on an understanding of the gaps and barriers in existing regulation)」。

例來說，針對特定較低風險產品採用縮減規模或簡化客戶審查（CDD）措施，或甚至於合理情況下豁免適用 CDD 措施³¹。G20 原則亦瞭解預付卡作為普惠金融工具的特定攸關性，因此建議針對其相關服務種類所存在的既有風險，制訂一特別的法規架構³²。符合比例之法規架構，可能開啟服務廠商以及未提供銀行業務／銀行業務活動甚少的區域加入市場。此方法亦可增加使用合法通路的情況，因此降低因遭金融體系排除而導致之 ML／TF 風險。

VI. 法規、監管與 RBA

88. 本節之指引，可協助各國處理於應用專屬 NPPS 之 FATF 建議時所將面臨的特定問題，並將於本節中檢視如何規範與監督與提供 NPPS 有關之實體、考量該等法規之影響，以及監督執行 AML／CFT 措施。

A. AML／CFT RBA 措施與監督

89. FATF 建議支持開發與執行 AML／CFT RBA。此 RBA 允許各國在 FATF 規定之架構下，採用更具彈性的措施，以更有效的運用其資源並採用與風險性質相關的預防性措施，並

³¹ 建議 IIN 第 6 條規定：豁免適用—各國得決定不適用部分要求金融機構或 DNFBP 採取特定行動之 FATF 建議，前提是...可證明 ML 及資助恐怖份子風險低，且僅應適用嚴格限制與合理之狀況，並與特定種類金融機構或活動有關...建議 IIN 完整內容，請參閱 www.fatf-gafi.org。

³² 符合比例原則之法規架構，可能包括（舉例來說）合併最高可允許交易金額、餘額門檻以及流動性與無力償債相關規定。

以最有效的方式執行相關努力。RBA 最重要的第一步是各國應首先依據建議 1 規定，辨識、評估與其所面臨之理解 ML 與 TF 風險，此為適用 FATF 建議規定之 AML/CFT 措施的最基本規定。另外，與此相關的規定還包括建議 15，要求各國與金融機構辨識與評估因開發新產品與新營運作業實務而可能帶來的 ML 或 TF 風險，包括針對新產品以及既有產品採用新交付機制以及開發新技術。各國因此必須採取適當與成比例的措施，以降低其發現的 NPPS 風險。

90. RBA 的一般原則是，若存在較高風險，則各國應要求金融機構採取強化措施管理及減輕該等風險，且因此風險較低時（且無可疑 ML 或 TF 活動），允許採用簡化措施。這代表各國能夠且應該摒棄「一體適用（one-size-fits-all）」的解決方案，並量身規劃符合其國家風險情況的 AML/CFT 法規架構。依據 RBA 規定，AML/CFT 措施之強度，視所辨識風險之程度與性質而定。RBA 要求各國針對較高風險領域採取更強化與集中的方法，並因此可對較低風險之部分採用簡化措施，以及針對可證明為低風險並符合其他條件之情況規範豁免適用規定。³³ 此等作法讓各國可在 FATF 規定架構下，採取更具彈性的措施，以更有效地運用其資源並採用與風險性質相關的預防性措施，並以最有效的方式執行相關努力。NPPS 之 RBA，另外使各國能夠減輕將

³³ 「低風險」狀況係指可能符合豁免 FATF 建議規定之情況，而簡化 AML/CFT 措施則可能適用「較低風險」之情況。

特定情況排除在金融系統以外的 ML/TF 風險，以及減輕達成有效執行 FATF 建議之障礙。

91. 如上所述，此 NPPS 風險基礎方法指引的目的，在依據及輔助既有 FATF 指引建立與開發及執行 AML/CFT RBA，尤其包括「FATF ML/TF 風險評估指引」，以及「FATF 防制 ML、TF 措施暨普惠金融指引」。

B. CDD

92. 依據建議 10 規定，各國應要求金融機構執行 CDD，以辨識其客戶及確認與客戶進行業務往來關係有關的資訊。CDD 規定之目的，在確保金融機構可有效辨識、驗證與監控其客戶以及其從事之金融交易，以及其可能帶來的 ML 與 TF 風險。
93. 依據建議 10 規定，各國應要求金融機構於下列情況下執行 CDD，包括辨識與驗證其之客戶身分：
 - (a) 建立業務往來關係；³⁴
 - (b) 偶爾執行金額高於 15,000 美元/歐元之交易，或進行建議 16 之註釋所規範電匯交易；
 - (c) 懷疑有 ML 或 TF 之情況；或
 - (d) 金融機構對先前取得身分識別資料之真實性與適切性有所懷疑。

³⁴FATF 建議並未定義此一概念，而是交由各國決定是否已建立業務往來關係。

94. 各國應考量的一個基本問題是，NPPS 是否與建立業務往來關係有關。通常，NPPS 的運作方式與建議 10 所述帳戶類似。為客戶持有與管理帳戶代表已建立業務往來關係，且應依據建議 10 規定執行 CDD 措施。開放式迴路可重複儲值預付卡，在其功能日益增多之後，其運作方式尤其將類似帳戶之運作方式。網路付款服務亦通常會代表其客戶持有與管理資金，而行動支付服務廠商，無論預付或後付，則通常也會與客戶建立建議 10 規範之業務往來關係。
95. 各國應要求金融機構承諾遵守符合建議 10 規定之 CDD 措施：(i)辨識與驗證客戶身分；(ii)辨識實質受益人；(iii)瞭解業務往來關係之目的；及(iv)持續監督業務往來關係。雖然各國應要求金融機構採用上述各 CDD 措施，不過其適用程度則需採用 RBA 決定。然而，另外亦需注意的一個重點是，就作為帳戶使用的 NPPS 而言，建議 10 規定各國不應允許金融機構開設匿名帳戶或以明顯假造的姓名開立帳戶。按 RBA 執行 AML/CFT 措施時，各國可考慮於新型態支付產品屬較低風險產品時適用簡化 CDD 措施。
96. 採用門檻為 CDD 與 NPPS 的重要考量因素。門檻可作為特定產品的有效風險減緩策略，因此可視為適用簡化 CDD 的措施。各國之門檻水準將依 NPPS 對該國所帶來的風險而定，且應依據風險評估結果決定。
97. 若 NPPS 屬較低風險且採用足夠的低儲值或使用限制規定，各國仍應要求金融機構適當注意為規避門檻與懷疑通

報規定所採取的偶爾為之及架構性計畫。舉例來說，各國應考慮採用門檻，使金融機構能夠使用客戶聲明執行 CDD 前三項步驟。就此方面，各國得考慮採用所謂「漸進式 (progressive)」或「分階段 (tiered)」KYC/CDD 方法，使低交易/支付/餘額上限措施能夠降低 ML/TF 風險。針對特定種類產品所設定的前述限制越嚴格，越能夠降低整體 ML/TF 風險，且該等產品/服務應視為較低風險產品。簡化 CDD 措施因此可能可適用。

98. 此外，就嚴格限制與證明屬低 ML/TF 風險之合理情況，各國得考慮豁免 NPPS 適用 CDD 措施³⁵。於此等情況下，特定低門檻可能可提供額外的防護。
99. 各國應確保 NPPS 廠商於持續採用 CDD 偵測可疑活動時，遵守 CDD 及監督規定。擁有與帳戶類似功能之 NPPS 的廠商，尤其應執行持續 CDD 作業。預付卡所擁有與帳戶類似之要素或功能越少，越可能適用簡化 CDD 措施。採用儲值限額可協助達到此等目的。
100. 各國應注意，FATF 建議允許金融機構於基本上不影響正常營運活動以及於 ML/TF 風險可有效管理的前提下，於建立業務往來關係後（而非建立業務往來關係之前或期間執

³⁵ 建議 IIN 第 6 條規定：豁免適用— 各國得決定不適用部分要求金融機構或 DNFBP 採取特定行動之 FATF 建議，前提是...可證明 ML 及資助恐怖份子風險低，且僅應適用嚴格限制與合理之狀況，並與特定種類金融機構或活動有關...建議 IIN 完整內容，請參閱 www.fatf-gafi.org。

行)，以非面對面方式驗證客戶身分³⁶。各國於建立業務往來關係後驗證客戶身分以決定應採行 CDD 之時點時，應將此點以及建議 10 之註釋納入考量³⁷。

101. 採用資金來源與交易上限規定，可減輕因採用零售賣場與網際網路經銷預付卡與行動支付服務時所帶來的風險。然而，在未執行適切 CDD 之情況下，透過網際網路購買預付卡可能使同一個人能夠使用不同姓名取得多張卡片。各國應考慮採取相關措施，降低於單筆交易中購買多份低於特定門檻之 NPPS（例如預付卡）以及向多個零售商購買的風險，通報可疑交易之規定應適用此等情況。各國亦應考慮對單筆交易出售之卡片數量設定限制，即使執行該等限制有其實務上的困難亦同。若預付卡或行動支付服務係透過零售賣場經銷，且該等零售商需執行 CDD 措施，則若賣場員工未經適切訓練，則亦可能產生錯誤辨識客戶的風險。若 CDD 作業是透過電子驗證執行，則廠商應確保其取得之資訊為正確並取自可靠來源。
102. 於大部分情況下，NPPS 廠商客戶很明顯的是申購服務或購買 NPPS 的個人。考量與 NPPS 客戶間有限或甚至並無面對面接觸的情況，NPPS 被交予未經廠商辨識之其他方或由該等其他方使用的風險便會增加。此等風險可透過採用強化

³⁶ 建議 10IN 第 11 條規定可能包括非面對面業務往來與證券交易的範例，且亦規定，金融機構將需針對客戶可能於驗證前就運用業務往來關係的情況採行風險管理程序。

³⁷ 請參閱建議 10IN 第 21 條規定。

措施執行持續 CDD 及交易監督作業的方式，依據 RBA 處理。或者，各國可考慮規定於其他交易時點執行 CDD，例如再儲值時。

103. 銀行與其他提供帳戶給 NPPS 廠商的存款收受機構所扮演的角色，是各國應予以考量的一個重要因素。各國應確保代替 NPPS 廠商持有資金的金融機構，依據建議 10 規定以及該等 NPPS 廠商所存在之風險考量，執行 CDD 措施。

C. 核准／登記

104. 於 NPPS 符合 FATF 建議之詞彙表所定義之 MVTS 時，廠商應依據 AML／CFT 措施規定取得核准、登記、受監督並遵守相關規定。建議 14 提供各國兩個核准或登記代理商的方式³⁸，各國應要求代理商取得核准或進行登記，或 MVTS 廠商應保存一份既有代理商之清單，並於權責機關要求時提供。
105. 以網路為基礎的 MVTS 必須遵守建議 14 之規定。若以網路為基礎的 MVTS 不在國境範圍內時，各國尤其應在法律與指引中清楚定義，適用實體 MVTS 之管轄區核准及／或登記要件，亦適用以網路為基礎的 MVTS，即使服務廠商的總部在境外亦同。此一問題將於以下章節中進一步討論。

³⁸ 依據建議 16IN 第 22 條規定，MVTS 廠商應於其直接或透過代理人營運之所在各國遵守建議 16 之所有相關規定。若 MVTS 廠商同時控制電匯的匯款方與受款方時，MVTS 廠商：(a)應將匯款與受款雙方的所有資訊納入考量，以決定是否應提交 STR；且(b)應於受可疑電匯影響的任何國家申報 STR，並提供相關交易資訊給 FIU。

D. 電匯

106. 建議 16 規範各國就電匯應遵守之規定。各國應確保金融機構於電匯時提供相關匯款人與收款人資訊，且該等資訊應依據建議 16 註釋之規定，於支付過程中隨時與電匯資料一同保存³⁹。此外，亦需針對匯出與收取電匯之客戶執行 CDD 措施。然而，很重要應注意的一點是，各國得針對跨境電匯規定微量（de minimis）門檻，低於門檻之交易將不需執行客戶與受益人資訊驗證作業，除非有 ML/TF 疑慮⁴⁰，亦即金額低於 1000 美元/歐元、偶爾為之的跨境電匯，將適用建議 16 註釋之規定，且將需提供匯款人與收款人名稱，以及帳號或獨特之交易參考號碼；然而，此等資訊將不需驗證。
107. 建議 16 適用跨境電匯及國內電匯⁴¹，且各國應決定此等規定是否適用 NPPS。提供個人間匯款功能之預付卡，擁有類似電匯之功能，因此需遵守建議 16 規定。建議 16 的目的並非規範以預付卡匯款購買產品與服務之交易，然而，若預付卡被用作個人間電匯交易的付款系統時，則其交易將適用建議 16 之規定⁴²。各國應規定發行作為個人間電匯交

³⁹ 為確保於跨國匯款時提供匯款人資訊，監理機關應運用專為跨國匯款而規定之篩選措施監督金融機構（而非國內匯款篩選）。

⁴⁰ 請參閱建議 16 IN 第 5 條。

⁴¹ 請參閱建議 16 IN 第 3 條。

⁴² 建議 16 之 IN 第 4 條規定：建議 16 的目的不在規範下列種類支付交易：(a) 任何為購買產品或服務而採用信用卡、扣款卡或預付卡所執行之匯款交易，前提是該等信用卡、扣款卡或預付卡的卡號於交易時一併提

易付款系統的預付卡之實體，需依據建議 16 規定提供與維護必要且正確的匯款人資訊，以及必要的受款人資訊及支付訊息。此外，屬 MVTS 廠商之行動支付服務及網路付款服務廠商，亦需遵守建議規定⁴³。

E. 監管方法以及辨識有權管轄區域

108. 各國應確保 NPPS 廠商依據建議 26 規定受到適切規範與監督。監理機關應採用 RBA，且屬 MVTS 廠商之 NPPS 廠商至少應取得核准或登記，並受有效監督系統之規範⁴⁴。
109. 就透過代理商經銷之 NPPS 而言，各國應確保採用代理商執行 AML/CFT 措施之實體，將該等代理商納入其 AML/CFT 計畫中，不得有任何例外，且應監督遵行情況。各國應確保於其法律架構下，NPPS 廠商仍需就其 AML/CFT 義務負責，且需就其代理商的行為負擔責任。
110. 建立監理架構時，各國應清楚規範負責監管 NPPS 廠商 AML/CFT 作業的權責機關。此外，監理機關應擁有足夠的權限，可監督或監控以及確保 NPPS 廠商依據建議 27 規定遵守 AML/CFT 規範。各國應依據市場狀況以及針對提

供。然而，當信用卡、扣款卡或預付卡是為作為進行個人間電匯交易之支付系統時，該等交易則應適用建議 16，且應將必要資訊納入電匯訊息中。完整建議 16IN 之內容，請參閱 www.fatf-gafi.org。

⁴³ 建議 16 之 IN 第 22 條規定：金錢或價值移轉服務（MVTS）廠商，應遵守其直接或透過代理人營運之國家相關規定。完整建議 16IN 之內容，請參閱 www.fatf-gafi.org。

⁴⁴ 請參閱建議 14。

供相同種類服務之實體採取一致監督方法等因素，考量規範與監督管轄區域內 NPPS 廠商之最適合且最有效率的主管機關，無論此等實體（例如：銀行、電信公司）間是否存在產業差異皆同。在許多情況下，權責機關可能很清楚。舉例來說，當一國對所有 AML/CFT 遵循行為設置單一權責機關。然而，於其他情況下，亦即各國考慮由不同權責機關監管不同 NPPS 廠商遵循 AML/CFT 規定之情況時，則建議制訂相關機制，協調相關權責機關之作業。

111. 行動支付服務方面，以 MNO 為主體的支付模式尤其重要，因為 MNO 通常並非由負責監管 AML/CFT 義務的公家機構所監管。舉例來說，各國可能考慮以相關通訊主管機關監管實體遵循 AML/CFT 之情況，尤其當大部分行動支付服務是由 MNO 所提供。然而，雖然通訊主管機關對行動產業理解較深入，且可能已監管相關 MNO，不過仍缺乏既有 AML/CFT 監管機關所擁有的 AML/CFT 專業。若以通訊主管機關為監管機關，則將需執行 AML/CFT 教育與訓練，以開發必要的專業知識。此外，金融與 AML/CFT 監理機關間亦必須密切合作，以確保就金融服務進行協調以及採用一致之作法。或者，可由既有 AML/CFT 主管權責機關在擁有 AML/CFT 專業的情況下，繼續監管行動支付服務廠商。應由哪一機關擔任行動支付服務之 AML/CFT 監管機關，將視各國相關環境以及既有監理機關架構而定。

112. 網路付款服務對各國執行 AML/CFT 法規與監管帶來了挑戰，因其跨境功能代表廠商能夠將總部設在與客戶所在國不同的國家。支付作業能夠在全球透過網際網路執行，且執法與監理機關將難以判定廠商是否確實於特定國家內進行營運活動。若廠商設立或未受適切 AML/CFT 法規管理與監管的管轄區域時，這點尤其需特別注意。各國應採取相關措施，確保於其管轄區域內提供網路付款服務的廠商皆遵守 AML/CFT 法規規定並受監管，無論廠商所在地為何皆同。各國尤其應依據建議 14 規定，要求 MVTS 廠商取得核准或進行登記，且應採取行動辨識於未取得該等核准或未登記之情況下執行 MVTS 之自然人或法人。為判定服務是否於特定國家提供，各國應考量相關網站就服務所使用之語言以及提供之敘述，於部分情況下，此等資料可能會顯示出服務廠商所鎖定的目標客戶族群。為協助監管於其管轄區域內所提供之服務，各國應考慮在其法律架構下⁴⁵，禁止網路付款服務廠商在管轄區域內無辦事處或代理商等實質營運地點的情況下，提供服務。

VII. 可處理風險的適當 AML/CFT 法規

113. 本節提供各國有關於決定哪一提供 NPPS 之實體應負責執行 AML/CFT 措施的指引，尤其與預付卡、行動支付服務及網路付款服務有關之部分。

⁴⁵ 法規架構之釋例，請參閱附錄 1（有關網路支付服務之部分）。

A. 與風險水準成比例之 AML/CFT 措施

114. 應執行 AML/CFT 措施之程度，應與 NPPS 具有之風險相符合。舉例來說，NPPS 功能與銀行帳戶功能越類似，越需適用類似之法規，包括應用完整 CDD 措施。尤其當 NPPS 功能與存款功能越來越類似時，更應適用類似的 AML/CFT 義務規定⁴⁶。
115. NPPS 功能與銀行帳戶功能類似的情況，可能具有下列一種或多種性質：
- (a) NPPS 可不限次數重複儲值；
 - (b) 未規範任何資金來源、儲值或支出限額或限額很高；
 - (c) 可跨境進行資金移轉與收款，亦可於產品發行國進行移轉；
 - (d) NPPS 可以現金付款，且現金可透過 ATM 網路提款；
或
 - (e) 可使用現金或現金等值物品對帳戶儲值或提領現金，無論係直接執行或其他廠商或中介機構。
116. 應用 AML/CFT RBA 之法規時，應將此等因子納入考量。各國監理機關就 NPPS 所採取之方法差異可能甚大，部分特定釋例請參閱附錄 1。各國於考量適用 NPPS 之

⁴⁶ 值得注意的是，符合比例原則以及量身規劃之方法，已經在 2011 年 10 月發表的「Wolfsberg 預付卡與儲值卡指導原則 (Wolfsberg Guidance on Prepaid and Stored Value Cards)」之私部門報告。本文件決定，預付卡與銀行帳戶間的關係越密切（例如：可儲值、無儲值/支出限制，且能夠移轉與收受資金），越需適用類似法規。

AML/CFT 措施時，可參考此等釋例；然而，各國最終仍應負擔於考量其相關環境與風險概況後，確保其 AML/CFT 法規架構符合 FATF 建議之責任。

B. 決定哪些 NPPS 廠商應遵守 AML/CFT 義務時應考量的問題

117. 考量可能參與提供 NPPS 之實體範圍廣泛，各國應確保其法律架構清楚規範監督與控管需符合 AML/CFT 規定之相關實體（以下合稱「NPPS 廠商」）的法律責任，並確保此等 NPPS 廠商依據建議 26 規定受到適切規範與監管。此外，符合 MVTS 廠商定義之 NPPS 廠商，應依據建議 14 規定之有效監督系統取得核准或進行登記並受其規範⁴⁷。

118. 如上所述，依據 FATF 建議，提供 NPPS 且屬 MVTS 或以 NPPS 作為支付方法之實體，應符合 AML/CFT 義務之規定。若有多個實體參與提供 NPPS 或服務，且不確定哪一實體為廠商，則各國於決定適當 NPPS 廠商時應考量下列因子：

- (a) 可清楚控制與管理 NPPS 之實體；
- (b) 與客戶維持往來關係之實體；

⁴⁷FATF 建議詞彙表規定：「MVTS 係指透過通訊、訊息、匯款或透過包括 MVTS 廠商之清算網路參與收受現金、支票、其他貨幣工具或其他價值儲存工具，以及以現金或其他形式支付予受款人之金融服務機構。此等服務廠商所執行之交易，可能包括一個或多個中介機構，以及最終支付款項予第三方，且可能包括任何 NPM。有時候，這些服務與特定地理區域有關，且以各種特定名詞敘述，包括 hawala、hundi 與 fei-chen。」

- (c) 自客戶取得資金之實體；及
- (d) 客戶向其求償資金之實體。

119. 依據營運模式之不同，尤其服務區隔清楚之部分，可能會有一個以上的實體負責提供 NPPS 並因此需符合 AML/CFT 之規定。下列針對預付卡、行動支付服務及網路付款服務提供進一步之指引。本指引尤其針對第 I 節所述參與提供 NPPS 之實體的營運內容與角色而規範。

i. 預付卡廠商

120. 於部分營運模式中，預付卡計畫係由依據與發卡機構所簽署契約規定提供支付服務之計畫管理公司有效執行，且發卡機構需對客戶之資金負責。於與客戶維持往來關係之期間，預付卡計畫管理公司應直接負責遵守 AML/CFT 法規規定，因其為清楚控管與管理提供預付卡服務之實體，或以發卡機構代理商身分間接受 AML/CFT 法規規範之實體。於其他情況下，發卡機構亦擔任計畫管理公司之角色，維持與客戶間之往來關係及監控卡片之使用。於此等情況下，發卡機構應遵守 AML/CFT 法規之規定。
121. 實務上，預付卡廠商通常運用其經銷商或代理商執行相關 AML/CFT 措施。於此等情況下，預付卡廠商很清楚地須負擔遵守 AML/CFT 措施之最終責任。預付卡經銷商於此等情境下，將代表 NPPS 廠商執行活動，且因此將視為預付卡廠商之代理商，無論預付卡是否視為 MVTS 皆同。於

此等情況下，預付卡廠商亦將需就因其經銷商或代理商之行為所導致未遵守此等 AML/CFT 義務之情況負責。

122. 於部分情況下，各國應考量對 NPPS 廠商及經銷商或代理商加諸 AML/CFT 法規之規定。於此法之下，經銷商或代理商將需承擔法律責任，且直接受相關監理機關監管。此方法於下列情況下尤其適用：經銷商與 NPPS 廠商間無契約關係，或實體位於難以有效監控該實體之其他國家。此情況常見於發卡機構使用批發經銷商，且該等經銷商亦採用大量經銷商或代理商之境。

ii. 行動支付服務廠商

123. 依據服務性質之不同，行動支付服務廠商因屬 MVTS 或發行與管理支付方法而符合金融機構定義。允許 P2P 移轉之行動支付服務廠商，係屬 MVTS，且各國應確保其受 AML/CFT 措施規範，包括與依據建議 14 規定取得核准或進行登記有關之部分。
124. 另一方面，提供 P2P 移轉功能之行動支付服務廠商亦符合 FATF 建議之規定範圍，因該等廠商係發行或管理支付方法之個體；AML/CFT 措施應適用此等廠商。然而，雖然各國可能選擇要求廠商取得核准或進行登記，仍應適用建議 14 之規定。
125. 應負責履行 AML/CFT 義務之實體，將依據行動支付服務之模式與架構而定。於以銀行為主體行動支付模式下，管

理資金及與客戶建立往來關係之銀行為金融機構，且需遵守 AML/CFT 措施之規定。

126. 於以 MNO 為主體之行動支付模式中，MNO 或其子公司為 FATF 建議所定義之金融機構。在此模式中，MNO 或其子公司提供服務、管理與客戶之關係、保管客戶資金，且客戶可對 MNO 或其子公司主張該資金之權益。
127. 如同預付卡，行動支付服務廠商可能採用各種經銷商擔任代理商，該等代理商透過 POS 直接接觸客戶，且將代表廠商執行 AML/CFT 措施（例如 CDD）。儲值預付款項至預付帳戶或發行行動貨幣便可能屬前述情況，於此等情境下，係由經銷商代表行動支付服務廠商執行活動，且因此需視為該實體之代理商，無論行動支付服務是否視為 MVTS 皆同。

iii. 網路付款服務廠商

128. 依據服務性質之不同，網路付款服務廠商因屬 MVTS 或發行與管理支付方法而符合金融機構定義。一般而言，網路付款服務廠商因允許 P2P 移轉而屬 MVTS。於此等情況下，各國應確保其受 AML/CFT 措施規範，包括與依據建議 14 規定取得核准或進行登記有關之部分。
129. 然而，部分發行電子貨幣作為產品與服務支付方法，且不允許 P2P 移轉之網路付款服務廠商，則因發行與管理支付方法而符合 FATF 建議之規定。AML/CFT 措施應適用此

等廠商，且雖然各國可能選擇要求廠商取得核准或進行登記，卻可能不適用建議 14 之規定。

130. 網路付款服務廠商為自客戶收取資金、貨幣與其他價值之實體，且：

- (a) 運用網際網路傳送支付訊息，以移轉或安排移轉資金、貨幣與其他價值至其他地點；或
- (b) 發行可用於移轉或支付款項之電子貨幣。

131. 雖然網路付款服務存在各種營運模式，但在一般情況下，提供服務之實體也管理與客戶間的往來關係。於此等模式下，客戶擁有對此等實體主張其資金之權利。各國應確保此實體負責履行 AML/CFT 義務並受監管。

附錄 1-NPPS 之監管方法

本附錄列示 FATF 會員國就 NPPS 相關事宜所採取監管方法之釋例。此等監管方法並未針對 2012 年 2 月通過之 FATF 建議進行評估，且其納入本指引文件並不代表遵循 FATF 建議規定。因此於本指引中列示，並不代表獲 FATF 認可。各國於考量適用 NPPS 之 AML/CFT 措施時，可參考此等釋例；然而，各國仍應負擔於考量其相關風險概況後，確保其 AML/CFT 法規架構符合 FATF 建議之責任。

預付卡

阿根廷

2011 年，阿根廷制訂了預付卡發卡機構適用的 AML/CFT 措施與程序（可重複儲值或不可重複儲值）。此等阿根廷法規規範了公司應就其客戶執行之 CDD 措施，且尤其要求各公司應逐月將發行金額超過 4,000 阿根廷披索（約 700 歐元）不可重複儲值預付卡的情況通報 FIU。

歐盟

歐洲制訂與預付卡（符合電子貨幣之廣義定義）有關規定的過程特別有趣 – 因其原本制訂、將電子貨幣視為與存款非常接近之法規架構，後來規定逐漸放鬆。此一結果透過於 2005 年

發佈「第三號 AML 指令 (third AML Directive)」並提出適用電子貨幣之簡化 CDD 架構的方式達成，後續則透過修訂適用可發行電子貨幣之機構的審慎法規架構執行，該等架構大幅度簡化原有的審慎規定，惟並未修訂基本 AML/CFT 義務規定。依據歐洲央行所提供的資料，合併此二法規架構以達促進歐洲市場電子貨幣開發的目標，獲致重大的成功。在歐元區中，以電子貨幣進行交易的數量，從 2006 年的 3,860 億歐元增加至 2010 年的 1,024,560 億歐元⁴⁸。然而，應該注意的是，封閉式迴路預付卡，亦即僅發卡機構接受之卡片，例如特定商家所發行之禮物卡，並未落在 EU 指令所定義的電子貨幣範圍內，封閉式迴路卡仍佔預付卡之大部分。

有趣的一點是，透過「第三號 AML 指令」推出了單一 EU 會員國適用簡化電子貨幣 CDD 措施的選項。該等措施係於諮詢市場營運廠商意見後提出，因市場營運廠商主張，將完整 CDD 措施套用到電子貨幣並不符合比例原則，因此也是電子貨幣市場採行該等措施的速度非常緩慢的原因。就市場需求面而言，市場存在需要快速與低成本的支付工具的正當需求，以協助可能無意願或沒機會開立銀行帳戶並使用支付系統的人（舉例來說：未成年人與移民）。截至 2004 年，全球政府也逐漸表現出改善匯款服務品質與降低價格的意願與承諾，電子貨幣產品（包括預付卡）似乎亦可達到此一目的。歐洲主管機關

⁴⁸ 請參「歐洲央行 (European Central Bank) (nc)」。

同意前述營運廠商的主張，並允許單一會員國於特定門檻之下適用電子貨幣簡化 CDD 措施：若電子貨幣無法重複儲值，為 150 歐元；且若電子貨幣可重複儲值，則年銷售額最高不得超過 2,500 歐元。於 2009 年發佈的第二份電子貨幣指令，將無法重複儲值之電子貨幣的門檻提高到最高 250 歐元。

註：FATF 確認，目前正在制訂「第四號歐盟 AML 指令（4th EU AML Directive）」中，且鼓勵讀者注意此一指令的發展與執行情況。

德國

應注意的是，部分 EU 會員國並未遵循「第三號 AML 指令」有關簡化 CDD 措施之作法，而是自行針對電子貨幣設計更嚴格的簡化審核規定。舉例來說，德國在 2011 年 12 月所推行的法令，僅允許於符合下列要件之情況下，方得立即與完全豁免預付卡產品適用 CDD 規定：

1. 產品門檻為 100 歐元（相較於 EU 指令，顯著較低）；
2. 產品並未賦予客戶執行個人間支付系統交易的權限；
3. 產品無法以其他電子貨幣產品重複儲值，且無法用於對其他電子貨幣產品重複儲值；且
4. 產品不允許提款超過 20 歐元現金。

不符合上述要件之預付卡，仍可因簡化 CDD 而獲益或甚至豁

免適用 CDD。然而，該等情況需向監理機關提出正式申請，且後者將評估個別預付卡產品之風險，並決定適用之 CDD 程度。此等風險評估作業並非完全依據門檻判定，而需將所有相關風險因子納入考量。另一方面，監理機關認定預付卡存在高 ML/TF 風險時，可指示發卡機構與經銷商並對發卡機構與經銷商採取額外措施，包括限制產品出售，此規定亦適用由境外營運公司發行之預付卡。

南非

在南非，會將來自發卡組織的預付卡發予部分工人支付薪資。預付卡可於 ATM 提領現金，或透過 POS 裝置購買產品。持卡人或其他外部各方，不得將額外資金（存款）上傳至預付卡，且不得針對此等卡片或員工之銀行存款餘額執行扣款命令。雇主可申請加入薪資計畫，於核准後，雇主需符合完整「金融情報中心法（Financial Intelligence Centre Act, FICA）」與 CDD 有關之規定，且需保存與各持卡人之身分與居住地址有關的紀錄。銀行接著會為雇主開立內部銀行帳戶，以供支付薪資，以及於任何時候反映預付卡所剩餘額。雇主需於發薪日之前，將薪資／報酬合計數匯入雇主之預付卡銀行帳戶，並將轉帳作業通知銀行，以及提供每張預付卡的匯款指示。

印度

銀行與非銀行實體所發行的預付支付工具（PPI），已成為印度

越來越受歡迎的支付方法。印度國內可發行的預付支付工具分為三種種類，亦即：(i)封閉系統支付工具；(ii)半封閉系統支付工具；以及(iii)開放系統支付工具。銀行及非銀行皆得發行 PPI，不過只有銀行可發行開放系統 PPI，亦即：可於 ATM 進行現金提款的 PPI。

銀行發行 PPI 之提案，經印度儲備銀行 RBI 相關主管部門審核後將獲得核准。所有提案經營包括發行 PPI 之支付系統的其他各方，皆須依據「支付與結算系統法（the Payment and Settlement System Act 2007）」取得印度儲備銀行（RBI）的授權。所有其他欲經營前述項目之人，最低資本額需達 1,000 萬印度盧比（INR）（約 18 萬美元），且自有資金淨額需為正。

任何類別 PPI 所允許之最高金額皆為 INR 50,000 元（約 900 美元）。合格 PPI 可透過現金及／或銀行帳戶扣款重複儲值，或以信用卡於銀行分行／ATM／授權通路／銀行代理商及非銀行實體刷卡儲值。獲授權銷售／重複儲值 PPI 之代理商，皆須經適當審查。

經 RBI 許可得提供行動銀行業務交易服務之銀行，得發行所有種類行動態樣 PPI（行動錢包與行動帳戶）。其他人則得發行以行動電話為基礎、金額上限為 INR 5,000 元（約 90 美元）的半封閉式 PPI，且不得提供任何可執行個人間價值移轉之設施。

銀行亦得依據「RBI 貨幣轉帳服務計畫（MTSS）」規定，針對跨國對內匯款之交易發行 PPI，且需符合 KYC 及其他條件規定。運用 PPI 執行跨國交易之行為，需遵守外匯管理規則之規

定。採用 RBA 作為預付支付工具的 KYC，是因為 CDD 的範圍因貨幣限額以及工具性質而將有所差異。銀行可發行下列三種半封閉式 PPI：

1. 於取得最低限度客戶資料之情況下，半封閉式系統預付支付工具最高可發行金額為 INR 10,000 元，前提是於任何時點的未償餘額不超過 INR 10,000 元，且任何月份之總儲值金額不得超過 INR 10,000 元。此等支付工具僅發行電子形式。
2. 於取得「洗錢防制法（the Prevention of Money Laundering Act）」第 2(d)條（Rule 2(d)）規定之「正式有效文件（officially valid document）」的情況下，半封閉式系統預付支付工具最高可發行金額為 INR 10,001 元至 INR 50,000 元。此等 PPI 僅發行電子形式，且不得重複儲值。
3. 於執行完整 KYC 之情況下，半封閉式系統預付支付工具最高可發行金額為 INR 50,000 元，且可重複儲值。

上述三種卡片皆可將資金移轉至相同發卡機構所發行之卡片，或移轉至取得許可之任何銀行帳戶。非銀行之實體，可發行以行動電話為基礎之半封閉式系統 PPI，金額上限為 INR 50,000 元（約 900 美元），此等卡片僅得用於國內交易。

發行 PPI 者需遵守「2002 年洗錢防制法（the Prevention of Money Laundering Act, 2002）」有關紀錄保存與通報之規定。

行動支付服務

歐盟

在歐洲，單一會員國得於符合下列門檻規定時，針對受規範之電子貨幣服務採行簡化 CDD：若電子貨幣無法重複儲值，為 250 歐元；且若電子貨幣可重複儲值，則年銷售額最高不得超過 2,500 歐元。此等條款適用資金預付之行動支付服務（於此等情況下，將視為電子貨幣），而非適用交易發生後之付款作業。

若所購買產品或服務符合「支付服務指令（Payment Services Directive）」與「第二號電子貨幣指令（Second Electronic Money Directive）」特定豁免規定時，則「直接發單收款（Direct Billing）」將豁免適用支付服務之規定。其中一個豁免規定是若產品或服務係透過行動電話購買並交付且用於電信、數位或 IT 裝置（例如：鈴聲、音樂或電子報），前提是 MNO 未擔任客戶與產品或服務供應商間之中介機構。

美國

美國採用之 AML/CFT 電子貨幣法規模型，同等看待所有新型態支付技術，不區分支付卡技術、行動技術或網路付款技術⁴⁹。若 MVTS 廠商於美國境內提供服務，則美國規定所有 MVTS 廠商皆應於美國取得核准與登記，無論其位於世界任何

⁴⁹ 美國法規稱電子貨幣廠商為預付存取服務之廠商與賣方。

地方。

印度

印度採用銀行主導的模式，除匯款外，另提供客戶存取銀行業務服務之權限。僅取得印度儲備銀行 RBI 核准與受其監督且於印度設有實質營運據點之銀行，得提供行動銀行業務服務。服務僅限提供予銀行客戶及／或扣款卡／信用卡持有人。客戶需向其銀行申請行動銀行業務，銀行於開始提供行動銀行業務服務前，需設置一套記載其客戶實質營運地點的文件登記系統。

由 National Payments Corporation of India (NPCI) 所開發與經營之「即時支付服務 (Immediate Payment Service, IMPS)」，亦可以行動電話為媒體，於不同銀行的不同帳戶間進行資金即時轉帳作業。惟該等服務僅適用以印度盧比計價之國內服務。

印度嚴格禁止提供跨國對內與對外匯款的行動銀行業務服務。

銀行亦可使用商業往來夥伴 (Business Correspondents, 即擔任實質銀行業務基礎架構延伸服務單位的個人及實體) 的服務，以將相關設施提供予其客戶。印度儲備銀行 RBI 不定時針對「認識您的客戶 (KYC)」、「防制洗錢 (AML)」以及「打擊資恐 (CFT)」所發佈的指引，亦將適用以行動為基礎的銀行業務服務。

銀行亦得提供行動銀行業務設施予其客戶，不受任何購買產品／服務之每日交易限額限制。若屬牽涉付出現金之資金轉帳，

則 Rs 10,000 元／（約 185 美元）之最高限額亦適用行動銀行。銀行可針對該等交易之速度規範適當上限規定，且每名客戶每月最高金額上限為 Rs 25,000／元（約 460 美元）。銀行應於指派相關人員擔任服務授權代理商前，針對該等人員執行適當審查作業。銀行需維持客戶帳戶之祕密與機密。

網際網路支付服務

阿根廷

「電子媒體支付」系統（MEP）之新法規，規定需辨識收受方與付款方之身分（包括稅務／勞工辨識號碼與帳戶 CBU）。匯款時有一標示付款人是否為 PEP 之欄位需填寫，此等作法將可對資金移轉進行控管，並將此納入為風險因子。MEP 係 BCRA（阿根廷中央銀行）經營之電子支付系統，通常用於大額交易作業。就此方面，提供網際網路支付服務之金融實體，需辨識收受方以及付款方，以及後者是否為 PEP。

歐盟

在歐洲，網路付款服務廠商於發行電子貨幣（「電子貨幣機構」）時需受「第二號電子貨幣指令（Second E-Money Directive 2009／110／EC）」所規範；或若於未發行電子貨幣之情況下提供支付服務（「支付機構」），則需受「支付服務指令（Payment Services Directive（2007／64／EC）」所規範。所有提供網路付款服務之授權支付服務廠商，皆須受完整 AML／CFT 措施之

規定。就以網路為基礎之預付帳戶方面，存放於該等帳戶之資金將視為電子貨幣，且因此於下列情況下將適用簡化 CDD：(i)若帳戶無法重複儲值，為 250 歐元；(ii)；且若帳戶可重複儲值，則年銷售額最高不得超過 2,500 歐元。依據「支付服務指令（2007/64/EC）」之護照條款（passporting provisions）規定營運之網路付款服務廠商，將可依據於一個會員國取得的授權，於全歐盟提供服務。該指令規定授權支付機構、其代理商與公司應進行公開登記，並將資料存放在支付服務廠商所在地之會員國，且要求會員國於監理之前提下互相合作，並將資訊提供予其他會員國負責授權與監管之權責機關。

就透過網際網路提供之支付服務方面，「電子商務指令（Electronic Commerce Directive）」（Directive 2000/31/EC）針對電子商務規範了內部市場架構，並為企業與消費者提供法律確定性。該指令允許所謂「資訊社會服務（information society services）」之廠商（亦包括透過網際網路提供之金融服務），依據其設立所在地相關法律規定，於全歐盟提供服務，不需於其他歐盟會員國設有實際營運據點，且原則上並不允許收受（或東道主）會員國對設立於其他會員國且提供跨境服務之公司加諸核准或登記義務。

美國

若 MVTS 廠商於美國境內提供服務，則美國規定所有 MVTS 廠商皆應於美國取得核准與登記，無論其位於世界任何地方。

此義務尤其適用於在任何地方無易於辨識營運據點之網路基礎 MVTS 廠商。

印度

僅取得印度儲備銀行（RBI）核准與受其監督且於印度設有實質營運據點之銀行，得提供網路銀行產品予印度居民。雖然開戶申請可透過網際網路收受，但銀行僅得於適當說明與實際驗證客戶身分後，方能開立帳戶。銀行需獨立保存與印度營運有關之資料，並於收到要求時，提供給 RBI 檢查／稽核。銀行需將每項違反安全系統與程序以及前述系統與程序故障之情況通報 RBI，且 RBI 得自行決定針對該等銀行執行特別稽核／檢查。就外匯交易方面，銀行需遵守與跨境交易、於印度境內操作與維護 vostro 帳戶有關之「外匯管理法（Foreign Exchange Management Act）」（FEMA）之規定。銀行需制訂適切風險控管措施，以管理風險與維持客戶帳戶之祕密與機密。

參考書目

- Relevant FATF material (all available at: www.fatf-gafi.org)
- FATF (2006), FATF Report on New Payment Methods, FATF, Paris
- FATF (2008), FATF Report: Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems, FATF, Paris
- FATF (2010), FATF Report: Money Laundering using New Payment Methods, FATF, Paris
- FATF (2012), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation - the FATF Recommendations, FATF Recommendations, FATF, Paris
- FATF (2013a), FATF Guidance on ML/TF risk assessment, FATF, Paris
- FATF (2013b), Guidance on anti-money laundering and terrorist financing measures and financial inclusion, FATF, Paris

OTHER USEFUL SOURCES:

- European Central Bank (nc), *Payment and terminal transactions involving non-MFIs, total number of transactions: 5. E-money purchase transactions*, www.ecb.int/stats/payments/paym/html/payments_nea_n_IEM.

NT.ZQZ.Z.en.html accessed on 22 June 2013.

- World Bank (2012), Innovations in Retail Payments Worldwide: A Snapshot.
- The Wolfsberg Group (2011), Wolfsberg Guidance on Prepaid and Stored Value Cards.

