Are the financial transactions conducted inside virtual environments truly anonymous?:An experimental research from an Australian perspective

Angela S M Irwin, Jill Slay, Raymond K-K Choo and Lin Liu
Forensic Computing Lab, Advanced Computing Research Centre
University of South Australia
Mawson Lakes, South Australia

Abstract

Purpose:This paper examines theidentity and payment method verification procedures implemented by a number of popularmassively multiplayer online games (MMOGs) and online financial service providers (OFSPs) to determine if the systems they currently have in place are sufficient to uncover the identities of those who may wish to use such environments to conduct money laundering or terrorism financing activity. The paper also investigates whether the payment instrumentsor methods used by account holders to place funds into their account(s) hinder or assist investigators to expose the real-world identity of the account holder. The paper then discusses whether it is feasible and/or desirable to introduce know your customer (KYC) and customer due diligence (CDD) legislation into virtual environments and illustrates an effective KYC approach which may assist MMOGs and OFSPs to correctly identify their account holders, should legislation be put in place.

Design/method/approach: Practical experiments were conducted with three popular MMOGs and fivepopular OFSPs to establish what information is collected from an account holder when an account is created and determine whether the information supplied at the account setup stage isverified in any way. The aim of these experiments was to ascertain whether it is possible to open accounts and place funds into virtual environments whilst maintaining high levels of anonymity. A number of fictitious individual (8) and business (2) personas were created in an attempt to open accounts and perform financial transactions with each of the MMOGs and OFSPs under investigation.

Findings: The systems currently in place by all of the MMOGsinvestigated are wholly inadequate to successfully establish the real-world identities of account holders. None of the information required at the account setup stage is verified and, therefore, cannot be reliably associated with an account holder in a real-world context. It appears that all three of the MMOGs investigated are leaving the serious matter of identity and payment method verification to the organisations that assist in the sale and purchase of their in-world currency such as third party currency exchanges and Internet payment systems (collectively referred to as OFSPs). However, many of these OFSPsdo not have adequatesystems in place to successfully verify the identities of their account holders or users either. Our experiments show that it can be a very simple process to open accounts and perform financial transactions with all of the OFSPs investigated using publicly available or fictitious identity information and a prepaid Visa® gift card. Although all five OFSPs investigated in this research claim to verify the identity of their account holders, and may already be subject to KYC and CDD legislation, their systems may need some work to ensure that an account holder or user is accurately identified before financial transactions can take place.

Originality/value: Although organisations that operate in virtual environments face significant difficulties and challenges in correctly identifying, verifying and authenticating their account holders, this paper proposes an electronic KYC approach that may be successfully used to circumvent many of these challenges. We believe that the electronic KYC approach discussed in this paper deals effectively with the challenges of global reach, anonymity and non-face-to-face business

relationships experienced by virtual environment operators, thereby assisting in the effective detection and possible prosecution of individuals who wish to use these platforms for illicit and illegal purposes.

Keywords: Anti-money laundering/counter terrorism financing (AML/CTF), virtual environments, know your customer (KYC), customer due diligence (CDD), electronic KYC approach

Classification: Research paper

1. Introduction

In recent years there has been much debate about the risks posed by virtual environments. Concern is growing about the ease in which virtual reality role-playing games, also known as Massively Multiplayer Online Games (MMOGs)[1], such as Second Life® and World of Warcraft® can be used for financially-motivated cybercrime, money laundering and terrorism financing (Tefft, 2007; Rijock, 2007; Sullivan, 2008; Methenitis, 2009; Sanders, 2009). Virtual environments are also reported to provide potential and opportunityfor allowing large sums of real and virtual currency to be moved across national borders without restriction and with little risk of being detected (British Broadcasting Corporation News, 2008; Heeks, 2008; Leapman, 2007; Lee, 2005). Currently virtual worlds and, more specifically,MMOGsare generally not subject to the laws and regulations of the real- world. Therefore, they may offer an excellent opportunity for criminals and terrorism financers to carry out their illegal activities unhindered and with impunity (Tefft, 2007). With Second Life® in particular, its fast-growing economy leaves many legal experts claiming that the lack of even basic regulation of its banks and stock exchange could provide a haven for money launders, fraudsters and terrorists to hide and move around funds to avoid the surveillance they would be subject to in the real world (Leapman, 2007).

The vulnerabilities that plague virtual environments are numerous but many of these vulnerabilities are compounded by the high levels of anonymity afforded to its users. For example:

1. The use of Avatars[2]which allows users to conceal their true identity when creating accounts and performing transactions.
2. The use of Internet cafes or public spaces, as pointed out by Brown, 2010, to accessvirtual environments and perform financial transactions.
3. The absence of KYC regulations whichremoves the onus fromMMOGs to correctly identify account holders before allowing them to move real and virtual funds through their account(s)(Brown, 2010 and Tefft, 2007.)
4. The ease in which it is possible to open accounts and perform financial transactions using stolen credit card numbers and prepaid Visa® or MasterCard® gift cards (Brown, 2010 andChoo, 2008[A]).
5. The global nature of virtual environments which allows the rapid and often informal transfer of real and virtual currency between players, accounts, OFSPs and across international borders, thereby making it extremely difficult to identify the true beneficial owner of funds.

[1]Also known as Massively Multiplayer Online Role-Playing Games (MMORPGs) and Massively Multiplayer Online Games (MMOs).

[2]An avatar is a computer user's representation of him or herself or alter ego, in the form of a three-dimensional model.

There can be no doubt that virtual environments provide high levels of anonymity to their users, but what is less clear is whether the OFSP, payment method or financial instrument selected to place funds into thevirtual environment or the anti-fraud and/or the anti-money laundering/counter terrorism financing (AML/CTF) measures in place by MMOGs and OFSPs can reveal the true identity of account holders. This research aims to shed light on these issues and make recommendations as to how virtual environment operators might make these environments less attractive as a platform for money laundering and terrorism financing activity.

This paper represents the findings of the third phase of a research project. The overall aim of the project, which is being undertaken in Australia, is to establish whether it is possible and/or feasible to launder money and raise funds for terrorism inside virtual environments (Anonymous, 2012[C]). The first phase of research involved the collection and statistical analysis of three hundred money laundering and terrorism financing typologies (Anonymous, 2012[A]). The statistical analysis phase attempted to measure the size of the money laundering and terrorism financing problem, identify threats and trends, the techniques employed and the amount of funds involved to determine whether the information obtained about money laundering and terrorism financing in real-world environments could be transferred to virtual environments. The second phase of research investigated how modelling could be used to provide an easy-to-follow, visual representation of the important characteristics and aspects of money laundering and terrorism financing behaviours (Anonymous, 2012[B]).This phase of research examines the account setup and account verification procedures carried out by a number of popular MMOGs and OFSPs. It also investigates whether the payment method used by an account holder to place funds into his or her account hinders or helps investigators to expose the identity of that account holder in a real-world context.

The rest of the paper is structured as follows: section 2provides a background to Australia's AML/CTF regime, including definitions of money laundering and terrorism financing and the motivation for money laundering and terrorism financing activity. It also looks at current KYCand CDD requirements for financial transactions which take place in real-world environments. These real-world KYC and CDD requirements will be used to determine whether the MMOGs and OFSPs under investigation have effective systems in place to accurately identify their account holders. Section 3discusses the research questions and describes the research methods used to answer these research questions. Section 4 presents the results obtainedand discusses whether the current account set-up and verification procedures utilised by the MMOGs and OFSPs are adequate for identifying those that might wish to use these environments for illicit or illegal activity; section 5 looks at whether it is feasible and/or desirable to introduce KYC and CDD legislation into virtual environments and discusses how MMOGs and OFSPs might become truly KYC and CDD compliant. An effective KYC approach, which may assist virtual environment operators to correctly identify their customers, is illustrated. Finally, section 6 concludes the paper.

2. Background: Australia's Anti-Money Laundering/Counter Terrorism Financing Regime

This section provides an introduction to money laundering and terrorism financing. It then looks at the importanceof effective KYC and CDD processes and procedures in determining the money laundering and terrorism financing risk posed by a customer. Since KYC and CDD requirements do not currently exist in virtual environments, we must look to real-world KYC and CDD legislation to determine what proper and effective KYC and CDD systems might look like. It is only then that we can determine whether the MMOGs and OFSPs under investigation have adequate processes and procedures in place to accurately identify their account holders.

2.1 Definition of and motivation for money laundering and terrorism financing

There are many definitions for money laundering, depending on whether you are looking at it from a legal, economic or social perspective. However, the definition applied to thisproject is the one used by the Australian Transaction Reports and Analysis Centre (AUSTRAC), Australia's AML/CTF regulator and specialist financial intelligence unit, which states that money laundering is "the process by which illegally obtained funds are given the appearance of having been legitimately obtained (AUSTRAC, 2012[A]). When a criminal activity generates substantial profits, the individual or group involved must find a way to control the funds without attracting attention to the underlying activity or the persons involved. Criminals do this by disguising the sources, changing the form, or moving the funds to a place where they are less likely to attract attention (Financial Supervision Commission, 2009).

There are generally three phases to money laundering: placement, layering and integration (FATF-GAFI, 2011). In the placement stage, the cash generated from crime is brought into the financial system. At this point the proceeds of crime are most apparent and at highest risk of detection. Money launderers 'place' the illegal funds using a variety of techniques, which include the deposit of cash into bank accounts and the use of cash to purchase high value assets such as land, property and luxury items.Once the proceeds of crime have been placed into the financial system, there is an attempt to conceal or disguise the source or ownership of the funds by creating complex layers of financial transactions. The purpose of this is to disassociate the illegal monies from the source of the crime by purposefully create a complex web of financial transactions aimed at concealing any audit trail and the source and ownership of funds. Integration of the cleaned money into the economy is the final stage of the process, and is accomplished by the launderer making it appear to have been legally earned. It is extremely difficult to discern between legal and illegal wealth at the integration stage.

Terrorism financing, on the other hand, occurs when the primary motivation is not financial gain but, rather, the use of funds to "encourage, plan, assist or engage in" acts of terrorism (WorldBank, 2003). Funds are often transferred using tactics that are progressively more complex. Terrorist financing networks operate globally and are able to gain access to the financial systems of both developing and developed countries.

There are three terrorism financing models: the Traditional Terrorism Financing Model (FINTRAC, 2009), the Reverse Terrorism Financing Model (AUSTRAC, 2009) and the Alternative Terrorism Financing Model (FINTRAC, 2009). They differ from the money laundering model in that terrorism financing funds can be from legitimate sources, not just criminal acts.

Although there can be a number of different motivators and drivers for money laundering and terrorism financing activity, they are inextricably linked. Terrorist groups usually have non-financial goals: publicity, dissemination of an ideology, the destruction of a society or regime, and simply spreading terror and intimidation. However, in practice, terrorists need finances and are often profit-oriented in addition to their ideological motivations (Hardouin, 2009).

Financial crime is a category which can generically encompass many others, like money laundering or terrorism financing or corruption or fraud. Clear links exist between terrorism financing, money laundering, cybercrime and traditional criminal activity (Nardo, 2006). The lines between fraud, money laundering and terrorist financing are blurred, and they should not be treated as separate events (Palmer, 2005). However, it is important to note that not all terrorism financing comes from illegal means; significant funds can be raised through legitimate businesses, fund raising efforts and donations. Equally, it must also be noted that money laundering and terrorism financing do not necessarily go hand-in-hand as a great deal of money laundering activity is for private profiteering

only and not for political purpose[3] (Choo and Smith, 2008). There has been a noted convergence between terrorism and organised crime since 9/11 (Choo, 2008[b]). The FBI, for example, noted that 'international organised criminals provide logistical andother support to terrorists, foreign intelligence services, and foreign governments, all with interests acutely adverse to those of U.S. national security' (FBI, 2008).

2.2 Know your Customer (KYC) and Customer Due Diligence (CDD) requirements for financial transactions taking place in real-world financial environments

KYC and CDD provisions are important requirements under the AML/CTFregime in Australia – see the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) (AML/CTF Act). The primary purpose of KYC and CDD provisions are to set out appropriate customer identification procedures for customers of a reporting entity as knowing a customer's identity and developing an understanding of the customer's expected financial activities are vital elements in determining the money laundering and terrorism financing risk posed by that customer.

The AML/CTF Act requires that reporting entities verify a customer's identity before a designated service (see Table 1) is provided (see section 6 of the AML/CTF Act) and that risks be assessed with regards to the type of customer that the service will be provided to, the type of designated service provided, how the designated service(s) will be delivered, the foreign jurisdictions that will be dealt with and whether the designated service will be offered by a permanent establishment in a foreign jurisdiction.

Sector	Service type
Financial:	Account/deposit-taking; financial services licence holder arranging a designated service; cash carrying/payroll; chequebook access facilities; currency exchange; custodial/depository; debit card access facilities; debt instruments; electronic funds transfers; lease/hire purchase; life insurance; loan; money/postal orders; pension/annuity; remittance services (money transfers); retirement savings accounts; securities market/investment; stored value cards; superannuation/approved deposit funds; travellers cheques exchange
Bullion:	Bullion dealing
Gambling:	Betting; betting accounts
Prescribed services:	Services specified in AML/CTF Regulations

Table 1: Classification of designated services, Section 6 of the AML/CTF Act

Under the AML/CTF Act, only new customers need to be identified, unless a suspicious matter reporting obligation arises in relation to an existing customer[3]. Where a suspicious matter reporting obligation does arise, the reporting entity must carry out applicable customer identification procedures[4], collect KYC information about the customer and verify, from a reliable and independent source, certain KYC information that has been obtained about the customer. All customers, new and existing, are subject to risk-based ongoing CDD procedures and each reporting entity must set out and define in its AML/CTF program its own set of triggers for collecting further KYC information, or verifying existing KYC information.

[3] Also known as a 'pre-commencement customer'

[4] Unless the reporting entity has previously carried out, or been deemed to have carried out, a customer identification procedure or comparable procedure.

Circumstances where a reporting entity may need to collect additional KYC information, or update or verify existing KYC information, include:

- a significant transaction or series of transactions (in amount, size or volume) has taken place which is inconsistent with the customer's profile or previous transactional activity conducted on the account
- a significant change occurs in the way that the account is operated by the customer
- doubts and/or suspicions exist about the identity of a customer

Under Australian AML/CTF KYC rules[5],the minimum applicable identification procedure for identifying an individual[6] is the collection and verification of the customer's full name and either thecustomer's date of birth or residential address. With respect to companies[7], at a minimum, the company's full name as registered by ASIC, the full address of the company's registered office, the full address of the company's principal place of business, if any; the ACN issued to the company; whether the company is registered by ADIC as a proprietary or public company and, if the company is registered as a proprietary company, the name of each director of the company must be collected and verified for identification purposes.Documents must be verified from reliable and independent documentation and/or reliable and independent electronic data(AUSTRAC, 2012[B]).

Before the introduction of the AML/CTF Act, the Financial Transactions Reporting Act 1988 (Cth) (FTRA) required that customers be verified using paper-based and face-to-face verification. However, the AML/CTF Act has introduced the acceptance of electronic verification, allowing a comprehensive and cost effective method of verifying new and existing customers without affecting levels of customer experience or service.

Where an individual is considered to be a medium or lower money laundering or terrorism financing risk, the AML/CTF rules provide for an 'electronic-based safe harbour procedure'. 'Safe harbour' is available to reporting entities if they collect the customer's full name, date of birth and residential address; and verify: (a) the customer's name and residential address using reliable and independent electronic data from at least two separate data sources; and either (b) the customer's date of birth using reliable and independent electronic data from at least one data source; or (c) that the customer has a transaction history for at least the past 3 years (ALRC, 2011).

Correctly identifying and verifying a customer from the outset is vital as failure to do so results in the subsequent ongoing CDD activity being of little or no value. However, customer identification controls are only part of ensuring that the true identity of a customer is established. Criminals (including money launderers and terrorism financers) are likely to have convincing falsified documentation; therefore human intervention is needed to ensure that systems and controls are routinely monitored and modified to identify abnormal behaviour.There are a number of things that may result in a customer being incorrectly identified. These include, but are not limited to:

- the legislation being incorrectly interpreted and applied;
- customer identification systems, policies and procedures not prompting for further identification if the money laundering or terrorism financing risk associated with a customer increases;
- systems not detecting that a customer has been insufficiently identified and allowing the customer to receive the designated services;

[5] See Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007, No. 1
[6] Parts 4.2 of the Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)
[7] Part 4.3 of the Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)

- inappropriate action being taken when a customer has provided insufficient or suspicious information for an identification check;
- accepting documents which cannot be readily verified (e.g. documents issued by foreign governments or entities);
- inappropriate action being taken when the document provided is neither an original nor a certified copy;
- not recognising when foreign identification documents have been issued by a jurisdiction considered to be high risk;
- accepting identity documentation that is expired or too old; and
- havinginsufficient access to information sources to help identify high-risk customers such as politically exposed persons (PEPs)[8], terrorists ordrug traffickers.

When a reporting entity has authorised another entity, such as an agent, to carry out customer identification, the legal responsibility for compliance with the customer identification provisions of the AML/CTF legislation remains with the reporting entity and cannot be passed to the agent. Therefore, it is important that customers are identified and verified correctly by all parties involved.

Under the FATF 40 recommendations[9] (FATF-GAFI, 2012), recommendations are set out stating that reporting entities must adopt adequate CDD and record-keeping procedures. However, the FATF 40 recommendations stipulate that financial institutions should pay special attention to any money laundering threats that may arise from new or developing technologies that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes. In particular, financial institutions should have policies and procedures in place to address any specific risks associated with non-face-to-face business relationships or transactions.

In section five we will discuss whether it is feasible and/or desirable to introduce KYC and CDD legislation into virtual environments and illustrate an effective KYC approach which may assist virtual environment operators to correctly identifying and verifying their customers from the outset.

3. Research methods

This sectiondescribes the research methods used to answer the primary research question addressed by this phase of research, namely, “Is it possible to open an accountwith a MMOG or OFSP and place funds into this account without revealing your real-world identity or source of funds”[10]?Section 3.1 details the experiment and review process. Section 3.2 provides an outline of the MMOGs and OFSPs selected for investigation. Section 3.3 provides an outline of the fictitious personas/companies created in order to carry out the experiments and also illustrates the MMOG and OFSP accounts opened by each of the fictitious personas and companies.

3.1 Experiment and review process

The research phase was split into two phases, review and experimentation, which were run concurrently.It should be noted that some of the research questions could not be fully answered by review alone, requiring instead a combination of review and experiment. For example, it is only possible to find out what personal information is required to open an account by actually opening an account.

[8]Politically exposed persons (PEPs) are individuals who are, or have been, entrusted with prominent public functions.

[9] Recommendations 10 and 11

[10] Secondary research questions are shown in Figure 1

During the review phase, specific information was gathered from each of the MMOGs and OFSPs under review(see Figure 1). The purpose of the information gathering exercise was to determine what personal[11] information was required to open an account and perform financial transactions, what payment methods were accepted for uploading funds to the account, what verificationchecks might be carried out on the information supplied by a new account holder and what KYC/CDD or broader AML/CTF and anti-fraud measures might be in place. The information gathered in the review process was used to assist us in the experimentation phase.

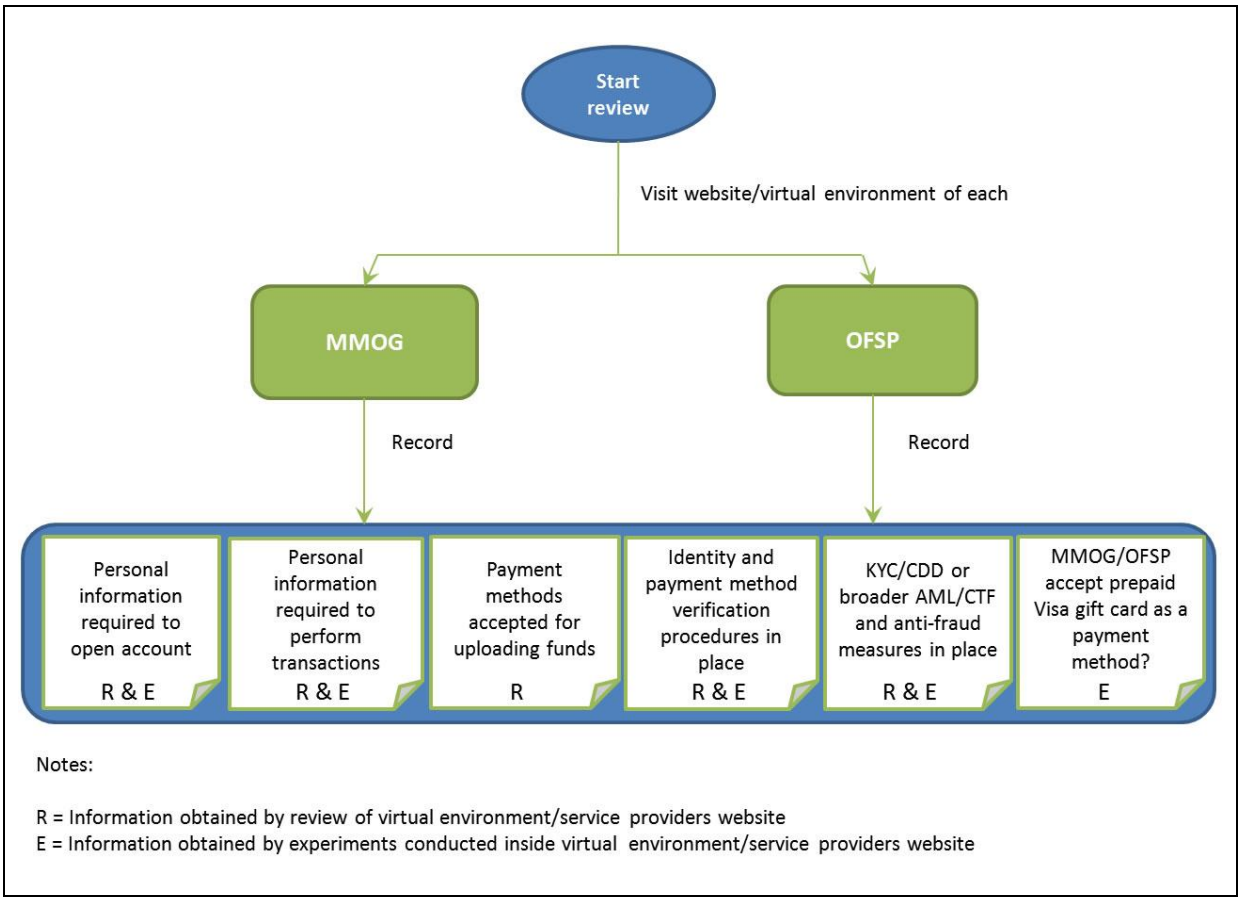

Figure 1: Information recorded during review phase (Source: Authors)

The experimentation phase aimed to ascertain whether accounts could be opened using false identity details (see section 3.3) and whether these accounts could be successfully funded using a prepaid Visa® or MasterCard® gift card or other type of anonymous payment system.We also wished to discover whether the verification checks that MMOGs and OFSPs claim to perform on new account holders were actually carried out. Figure 2 shows the steps involved in the experimentation phase.

[11]For example, name, date of birth, residential address etc.

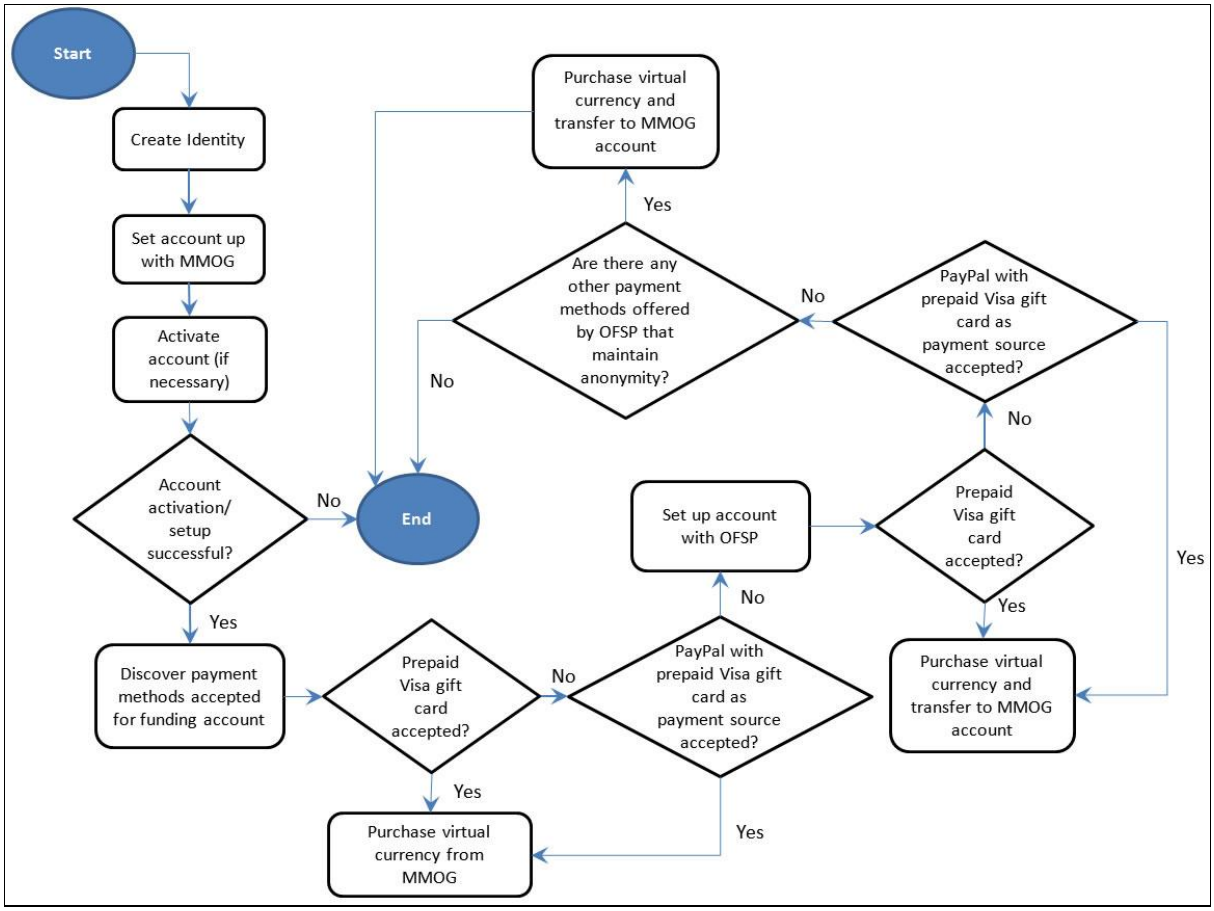

Figure 2: Steps involved in the review and experimentationprocess (Source: Authors)

3.2 Outline of MMOGs and OFSPs investigated

Only MMOGs that possessed their own internal economy and/or in-world currency which could be purchased and sold inside the virtual environment itself or traded using a number of OFSPs were selected for review and experimentation and only OFSP that could be used to place funds into these virtual environments, either directly or indirectly, were selected for account creation. The following paragraphs provide brief details of the MMOGs and OFSPs selected. The real identities of the MMOGs and OFSPs have been concealed to ensure that the contents of this paper are not misused. However, we can provide the dataset to law enforcement or other agencies/entities upon request.

MMOGs

MMOG 1 allows account holders to create and trade virtual property and services with one another. It has its own internal currency which can be used to buy, sell, rent or trade land or goods and services with other account holders. The currency inside MMOG 1 can be traded for real-world cash or can be exchanged for other virtual currencies using a number of virtual currency exchanges. MMOG 1 is free to use, however, account holders can purchase a premium membership package which gives them access to increased levels of customer support and other membership benefits. If an account holder wishes to perform financial transactions through his or her account, he or she must add contact and billing details to his or her account profile. MMOG 1 provides four different account types - resident, business owner, enterprise and currency trader. Experiments were conducted using the resident account type.

Similar to MMOG 1, MMOG 2 is a virtual reality space which is created by its account holders. Account holders meet to chat, create virtual goods or places, learn or socialise. MMOG 2 has an

active and diverse economy where account holders can create and sell goods and services to other account holders. The currency inside MMOG 2 can also be traded for real-world cash or exchanged for other virtual currencies using a number of virtual currency exchanges. MMOG 2 is free to use, however, users must be over 18 years of age.

MMOG 3 is an online virtual social entertainment destination in which account holders can meet new people, chat, create, and play games. Like the other twoMMOGs investigated, MMOG 3 has an active economy where account holders can create and sell goods and services to other residents. MMOG 3 contains its own economy with a currency system based on credits, promotional credits and developer tokens[12]. Account holders can purchase in-world credits using real-world currency either directly from MMOG 3 or from third party resellers. Credits may also be purchased on gift cards available from retail outlets such as department stores.Unused credits cannot be returned to MMOG 3in exchangereal-world currency but can be sold to registered resellers who will purchase them for real-world currency. The credits are used by account holders to purchase virtual items such as clothing, pets, property and land. Promotional credits can be obtained by participating in partner promotions. Promotional credits are similar to standard credits in that a given number of promotional credits equates to the same number of standard credits, however, promotionalcredits cannot be traded back to MMOG 3 for actual currency. Promotional credits are used to purchase virtual products and are exchanged into developer tokenswhen the transaction takes place. Developer tokens, however, are not equal in value to promotional credits as developers receive only a single developer token per purchase, regardless of the price of the product purchased. Content creators earn credits when their items are sold and are allowed to resell the credits they earn, through an approved trusted reseller, as they cannot be resold to MMOG 3 itself. Developer tokens appear only if an account holder pays a developer for a custom item using promotional credits instead of standard credits.

OFSPs

OFSP 1 is an e-commerce business that allows payments and money transfers to be made through the Internet. Originally, an OFSP 1 account could be funded with an electronic debit from a bank account or by a credit card but in 2010, OFSP 1 began to require that a verified bank account be used after the account holder exceeded a predetermined spending limit.

OFSP 2 is an Internet payment and eWallet service with over 16 million account holders worldwide and provides more than 100 payment options, with 41 currencies covering 200 countries and territories. OFSP 2 enables account holders to make online payments conveniently, securely and economically.

OFSP 3allows account holders to make and receive payments instantly via the Internet. OFSP 3 account holders can convert national currencies (i.e. cash) to OFSP 3's currency; convert OFSP 3's currency to most national currencies and convert OFSP 3's currency to gold and gold to OFSP 3's currency. OFSP 3 does not sell its currency directly to account holders, instead, it uses numerous virtual currency exchangers to assist account holders to put value into their OFSP 3's account or convert OFSP 3's value back into their national currency. All virtual currency exchangers used by OFSP 3 are independent businesses which are not affiliated with OFSP 3.

OFSP 4 is an independent, online virtual currency exchange where customers can buy, sell and exchange a number of virtual currencies. OFSP 4 also provides debit cards where funds can be transferred from a customer's electronic accounts straight to cash and withdrawn in local currency at an ATM machine. These debit cards can be used at most ATMs worldwide.

[12] Developer tokens are for account holders who sell custom-made items. Developer tokens are earned when an account holder purchases an item with promotional credits.

OFSP 5 is one of the leading European exchanges for a number of virtual currencies. OFSP 5 allows account holders to buy and sell a number of virtual currencies in exchange for EUR, GBP, CHF and USD and vice versa.

3.3 Outline of fictitious personas and fictitious companies

This section provides an outline of the fictitious personas and companies that werecreatedin order to carry out the experimentation phase of research.

Eight fictitious individual and two fictitious business personaswere created (see Figure 3). These personas were used to open accounts with MMOGs and OFSPs, perform financial transactions andwould be used to represent the entities and actors involved in the virtual money laundering or terrorism financing activity in the later stages of research. Each of the individual personas were given a gender, name, date of birth, postal address and email address[13]and were set up using the following criteria: a mixture of male and female genders; names that may be associated with a particular ethnicity; dates of birth ranging from 1949 to 1988; postal addresses from a wide range of countries and email addresses that were set up with service providers that do not require verification of the details entered at account set up.

To provide some level of credibility to the postal addresses allocated to each of the personas, Google Maps™ and the equivalent of the Australia Post™ postal code finder were used to find potential addresses for each country. Although the street, town and city names used for our personas were real, the door numbers that were used to construct the addresses were not. For example, the Australia Post™ postal code finder may show that the numbers 1 – 195 Main Street, some town, in some city exists. Therefore, the address allocated to one of the personas would be 196 Main Street, some town, in some city, which does not exist. This ensured that no real-world address, belonging to a real-world person could be affected by our research.

Of the two businesses personas created, one business resembleda real-world business based in North America and was used in an attempt to obtain a business account from one of the OFSP's. Publicly available information about this real-world business was used to determine whether a business account could be successfully created with the OFSP. However, no funds were uploaded to the business account and no financial transactions were performed using the account. After completing the experiments, we wished to make the account unusable; therefore, we deliberately entered a wrong password three times, resulting in the account being frozen by the OFSP.The second business, which was wholly fictitious, was used to attempt to obtain a business account from one of the MMOGs. This business account will be used in future experiments to carry out layering transactions and techniques which aim to confuse or obfuscate the money trail.Business accounts were opened because they normally attract higher transaction limits than personal accounts- an important aspect in discovering whether it is feasible to use MMOGs and OFSP for money laundering and terrorism financing activity. In addition, moving funds through business accounts is a common money laundering and terrorism financing technique.

Figure 3 shows the role of each of the fictitious personas, the personal attributes[14] assigned to the individual andthe MMOG and OFSP accounts that were successfully created using the fictitious persona details.

[13] Full details of the fictitious identities have not been provided on Figure 3 in order to protect the identity of the Avatars and accounts created.

[14] Some of the attributes have not been disclosed to ensure that they cannot be identified

Entity	Successfully opened accounts with:	
Suspect 1 Sex: Male; Location: France; DOB: 24/4/1981	MMOG 1	OFSP 1
Suspect 2 Sex: Male; Location: UK; DOB: 13/12/1986	MMOG 1	OFSP 1
Suspect 3 Sex: Female; Location: USA; DOB: 23/2/1973		OFSP 2
Third Party Sex: Male; Location: USA; DOB: 15/5/1988	MMOG 1	OFSP 5
Accomplice 1 Sex: Male; Location: Pakistan; DOB: 25/11/1966	MMOG 1 MMOG 3	OFSP 3
Accomplice 2 Sex: Male; Location: Germany; DOB: 28/10/1965		OFSP 2
Beneficiary 1 Sex: Female; Location: UK; DOB: 27/2/1977	MMOG 1 MMOG 2	OFSP 5
Beneficiary 2 Sex: Male; Location: Australia; DOB: 5/10/1949	MMOG 1 MMOG 3	OFSP 1 OFSP 2 OFSP 4 OFSP 5
Business 1 Type: Florist; Location: Germany		
Business 2 Type: Restaurant; Location: USA		OFSP 2

Figure 3: Accounts created with MMOGs and OFSPs (Source: Authors)

4. Results

This section discusses the results of the review and experimentation phases of research. The results for the MMOGs and OFSPs are treated separately. However, it should be noted, that in some cases, it was necessary to open a MMOG and OFSPs together in order to carry out some of the fund transfer experiments.

4.1 MMOGs

4.1.1 Personal information required from an account holder to open an account

As can be seen from Table 2, the only real-world information required to open an account with each of the MMOGs investigated is an email address.This is wholly inadequate as the minimum level of information required to successfully verify an individual's identity is their full legal name and date of birth or residential address.

Section ID		MMOG 1	MMOG 2	MMOG 3
4.1.1	Personal information required from an account holder to openan account:	Resident account: • Choose an avatar • Choose a username • Email address • Date of birth • Password • Security question	• Enter a first name • Choose a last name • Select an avatar • Email address • Password	• Choose an avatar • Choose an avatar name • Create a password • Enter first name • Enter last name • Enter email address • Enter country

		• Security answer		• Enter date of birth
4.1.2	Identity verification procedures	None	Verification link sent to email address provided	Verification link sent to email address provided (link verification is optional)
4.1.3	Personal information required to perform financial transactions:	Contact address and billing details	N/A – must go through payment service provider	N/A - must go through payment service provider
4.1.4	Payment method verification procedures	Carried out by payment service provider	Carried out by payment service provider	Carried out by payment service provider
4.1.5	Payment methods offered (for uploading funds)	PayPal®, Credit card	PayPal®, IcePay® – Visa®, PaySafeCard® and Wire Transfer	Credit card, PayPal®, Google Checkout™, Pay by cash, BPAY© Wallie-card, Click & Buy, Western Union®, Echeck, Boku™ Pay by Mobile™
4.1.6	Other KYC/CDD, AML/CTF or anti-fraud measures in place	None found	None found	IP address recorded
4.1.7	Can financial transactions be carried out using unverified payment methods?	No	Yes[15]	Yes

Table 2: Identity verification and payment method confirmation procedures carried out by the MMOG under review

4.1.2 Identityverification procedures performed by MMOGs

Although an email addresswas requested by MMOG 1, experimentation found that no verification was performed on the email address supplied as an email address made up of nonsensical characters and an email address that did not exist were accepted by MMOG 1 when setting up two of the accounts. In addition, no account activation procedures, in the form of an email verification link were carried out by MMOG 1, had this been the case, this may have flagged to MMOG 1 that an incorrect or non-existent email address had been used and the accounts could have been deactivated or frozen. A valid email addresses must be supplied when opening accounts with MMOG 2 or MMOG 3 as this email address is used to send an account verification link[16].

Although verifying an email address provides some level of identity confirmation, this alone cannot be relied upon to verify a person's identity as there are many companies that provide email accounts free of charge without requiring the account holder to go through any form of identity verification procedures to obtain one.

The procedures currently in place by all MMOGs to verify the identity of their account holders are wholly inadequate. None of the information requested at the account setup stage can be reliably verified and, therefore, cannot be reliably associated with an account holder in a real-world context. If each of the MMOGs had collected sufficient information at the account setup phase, they could

[15] See section 4.1.7 for further details.

[16] Verification of the email address supplied to MMOG 3 is optional. However, the account holder earns free credits by doing so.

have checked the information provided against a number of public databases to ensure that the person existed and the information that they had supplied was correct.

4.1.3 Personal information required from an account holder to perform financial transactions

In order to transfer funds or perform financial transactions inside MMOG 1, the account holder must add contact details in the form of full name and residential address and billing details in the form of credit card details (card type, card number and expiration date) or a verified PayPal® account (PayPal® email address and PayPal® password)to his or her account profile. Although MMOG 1 collects billing details from account holders, virtual currency must be purchased or sold via their internal virtual currency exchange service (IVCES) or through a number of OFSPs.

There was nowhere on the MMOG 2 or MMOG 3 Account Managerscreen for contact or billing details to be added. Therefore, if the account holder wishes to purchase virtual currencyhe must do so using a third party OFSP (see Table 2).

4.1.4 Payment method verification procedures enforced by MMOG

Only one of the three MMOGs investigated (MMOG 1) required account holders to provide their full name, residential addressand payment details to perform financial transactions. However, experimentation shows that no verification checks are carried out on the contact or billing details entered as we were able to successfully create a number of avatar accounts using the contact details of six of our fictitious personas[17]. No effort was made to determine whether the individual resided at the address provided, or that the address even existed. In addition, we were able to add a verified PayPal® account, which was set up in the name of one of the fictitious personas, as a valid payment method to a number of the fictitious MMOG 1 avatar accounts.

It appears that all three MMOGs investigated are leaving the serious matter of identity and payment method verification to third party exchanges (such as IVCES) and the organisations that assist in the sale and purchase of their in-world currency such as credit card companies and Internet payment systems. However, as will be discussed later in this paper, many of these organisations may not have adequate processes or procedures in place to successfully verify the identity of their account holders or users.

4.1.5 Payment methods accepted by MMOGs for uploading funds

As can be seen from Table 2,MMOG 1 accepts only PayPal® and credit card details as payment options for adding funds to an avatar account. MMOG 2 accepts PayPal® and Visa®, PaySafeCard® and Wire Transfer using their IcePay® system. MMOG 3 accepts the widest range of payment methods, including credit card, PayPal®, Pay by Cash, Western Union® and BPAY©.The type of payment methods accepted by each of the MMOGs is important for account holder identification purposes as they may provide a possible avenue to discovering the real-world identity of an account holder, due to the types of information that may be disclosed about an account holder when a financial transaction is performed. For example, a lot can be learned about an account holder if he or she uses a credit card to make a transaction. However, if the account holder uses a Pay by Cash facility such as UKash®, very little can be learned about the account holder as no personal details are required to purchase anUKash®PIN.

Table 3 shows the levels of anonymity afforded to the payment methods accepted by each of the MMOGs investigated.

[17] A fictitious persona can have one or more avatar accounts.

Payment Method	Level of anonymity	
	High	Low
PayPal®		√
Credit card		√
IcePay® – Visa®		√
PaySafeCard®[18]	-	-
Wire Transfer		√
Google Checkout™[19]	-	-
BPAY©		√
Wallie-card[20]	-	-
ClickandBuy	√	
Western Union®		√
Echeck		√
Boku™ Pay by Mobile™		√

Table 3: Levels of anonymity afforded to payment methods offered by MMOGs investigated

As can be seen from Table 3, only the ClickandBuy payment method offers high levels of anonymity. This is because a user can set up their account using false identity details and link a prepaid Visa® or MasterCard® gift card to their account. Allowing a prepaid Visa® or MasterCard®gift card to be added to an account as a valid payment method results in the financial trail being lost as these cards can be purchased at millions of outlets worldwide using cash and without the need to show any form of identification.

In some situations BPAY©can offer high levels of anonymity. However,to use the BPAY© facility offered by MMOG 3, the user must register for telephone or Internet banking with his or her financial institution. A BPAY© payment can be made at the user's financial institution using a cheque, savings or credit card account. To make a BPAY© payment, the account holder selects the Pay by Cash method and the number of credits he or she wishes to purchase. The account holder then adds his or her contact details into an online form - this contact information is used to match up the payment with the order. Once the online form is processed, payment instructions are displayed on the screen. These payment instructions must be added to a bank transfer form and presented to the account holder's bank or by logging into the Internet or phone banking service and making a payment. The BPAY© system would not be the best way to add funds to the virtual environment as the account holder would be required to reveal their bank account details, thereby, reducing the level of anonymity afforded to the transaction.

BPAY© comes under the umbrella of a Pay by Cash facility. Another common Pay by Cash facility is UKash®[21]. UKash®works by physically exchanging cash at a sales outlet in return for a PIN number. The PIN is loaded with the amount handed over to the sales outlet and can be used to make purchases online, including buying virtual currencies. Each time an online transaction is made, the amount is deducted from the Ukash® balance. No personal details are required to purchase the UKash® PIN. If a user wishes to pay for larger amounts, he or she can combine up to 10 PINs per payment process and pay for items up to GBP 1,000 or AUD 1,554 in a single transaction. This gives the PIN holder access to GBP 1,000/AUD 1,554 of untraceable funds. However, in reality, the UKash® systems can be used to anonymously move larger sums of money online and through virtual

[18] PaySafeCard® is not available in Australia therefore this could not be tested.
[19] Google Checkout™ is not available in Australia therefore this could not be tested.
[20] Wallie-card is now discontinued and rebranded under PaySafeCard®
[21] UKash®was not offered as a payment method by any of the MMOGs investigated.

environments as there is no way to keep track of how many PINs that an individual has purchased, especially if the individual has numerous personas or identities. The UKash® system is an effective way to get funds into the virtual economy with little or no risk of uncovering the true identity of the depositor or source of funds.

Under normal operating conditions the other payment methods offer low levels of anonymity because they require account holders or users to supply their credit card, bank account or landline/mobile telephone[22]details.The only way that the level of anonymity of these payment methods could be increased is if they allowed either a prepaid Visa® or MasterCard® gift card to be added as a valid payment method or stolen credit card details were used to set up the account and carry out the transaction. Section 4.1.7 investigates the use of prepaid Visa® gift cards to set up accounts and/or carry out transactions in greater detail.

4.1.6 Other KYC/CDD, AML/CTF or anti-fraud measures in place by MMOGs

MMOG 3 appears to carry out some kind of CDD activity as an unsuccessful attempt was made by Accomplice 1 to purchase 5,000 credits using one of the prepaid Visa® gift cards as a payment method. When the order was processed the following message was displayed on the screen:

> *"Your order has been sent to a specialist for further review. This process should take approximately 1 – 2 business days. During this time, any other orders you place will automatically be sent for review as well. We appreciate your patience during this time".*

To test whether the issue was related to the use of a prepaid Visa® gift card as a payment method, a new account was created for Beneficiary 2 and a different prepaid Visa® gift card was used to purchase credits. Funds were successfully added to the new account using the prepaid Visa® gift card. Therefore, the account was flagged for further review for some other reason and not because a prepaid Visa® gift card was being used.

This account may have been triggered for review for a number of reasons, including:

1. Although account holder purportedly came from Pakistan, the transaction was being carried out in Australia (without using privacy enhancing software). Therefore, it is possible that the IP address was being recorded during this transaction and the discrepancy was picked up.
2. A postal code of 0000 was added to the postcode field as we did not have a postal code for this specific address in Pakistan.
3. The prepaid Visa®gift card was issued in Australia and not Pakistan as would be expected from a Pakistani account holder.
4. Pakistan might be considered as a high risk country therefore all transactions performed from this region may be subject to special review.

MMOG 3 records the IP address of the account holder when setting up an account. However, IP addresses can be successfully concealed using privacy enhancing software such as Tor Browser software, therefore, cannot be relied upon to reliably verify the account holder's identity or location.

[22] MMOG 3 allows credits to be purchased using the account holder's landline or mobile phone and the charge for the purchase appears on the account holder's next telephone bill (landline or contract mobile phone) or is immediately debited from the balance (prepaid/pay-as-you-go mobile phone). When a user attempts to purchase credits using a telephone, he or she is asked to confirm the purchase via text message before the transaction is finalised.

Originally designed, implemented and deployed as a third-generation onion routing project of the U.S. Naval Research Laboratory, the Tor project[23] was developed for the primary purpose of protecting government communications. Today, it is used every day for a wide variety of purposes by normal people, the military, journalists, law enforcement officers, activists, and many others, including criminals[24]. Tor is a network of virtual tunnels that allows people and groups to improve their privacy and security on the Internet. One of the reasons that individuals use Tor is to keep websites from tracking their movements on the Internet; known as 'traffic analysis', a common form of Internet surveillance. The variety of people who use Tor is actually part of what makes it so secure. Tor works by hiding the user among the other users on the network, so the more populous and diverse the user-base for Tor is, the greater the level of anonymity.

No other KYC/CDD, anti-money laundering or anti-fraud measures were discovered during the MMOG experimentation phase.

4.1.7 Can anonymity of a payment method accepted by a MMOG be increased by utilising a prepaid Visa®/MasterCard® gift card as a payment source?

A number of experiments were carried out to determine whether some of the payment methods classified as offering low levels of anonymity (see Table 3) could be increased to offer higher levels of anonymity by attaching a prepaid Visa® gift card as their payment source.These experiments were conducted using both the fictitious personas and the accounts set up with theMMOGs and OFSPs.The results of the experiments are as follows:

PayPal® will accept a prepaid Visa® or MasterCard® gift card as a primary payment source. However, each of the attempts to purchase in-world currency from the IVCES linked to MMOG 1 using a PayPal® account with the primary payment source being a prepaid Visa® gift card failed. The IVCES was able to recognise that the verified PayPal® account was using a prepaid Visa® gift card as its main payment source and declined all of these transactions. A number of theother OFSPs investigated, however, accepted both the prepaid Visa® gift card and the verified PayPal® account as valid payment methods, and these OFSPs were used to successfully transfer funds to all of the fictitious avatar accounts set up with MMOG 1.For example, an account was set up with OFSP 5 in the name of Beneficiary 2. A PayPal® account, with a prepaid Visa® gift card as the primary payment source, was added to Beneficiary 2's OFSP 5 account as a payment method. In order to purchase the in-world currency of MMOG 1 from OFSP 5, USD 20 was successfully credited to Beneficiary 2's OFSP 5 account from the PayPal® account. The next step was to convert the USDs to MMOG 1's in-world currency - this was done using Beneficiary 2's OFSP 5 account. The final step was to transfer the MMOG 1 in-world currency being held in the OFSP 5 account to the Beneficiary 2's MMOG 1

[23] See https://www.torproject.org/about/overview.html [last accessed: 30 April 2012]

[24] In September 2011, for example, eight individuals were charged for operating a secret online store that reportedly sold more than USD 1 million worth of narcotics. It was alleged in the 12-count indictment that '[i]n approximately January 2010, to improve anonymity, the operators moved their on-line controlled substances marketplace to the TOR network … On the TOR network, the on-line controlled substances marketplace was called "The Farmer's Market." The majority of communications between the operators, sources of supply, and customers occurred on The Farmer's Market website via internal private messaging. The on-line marketplaces have accepted Western Union, Pecunix, PayPal, I-Golder, and cash as payment for illegal drug sales. Customers who paid in cash for their orders sent the cash to addresses controlled by a co-conspirator. The co-conspirator then collected the cash and forwarded the cash, minus a commission, to the operators via Western Union or other means. The organization referred to the addresses used to accept these cash payments or individuals who accepted these cash payments as "cash drops."' – see *United States of America v. Marc Peter Willems, Michael Evron, Jonathan Colbeck, Ryan Rawls, Jonathan Dugan, Brian Colbeck, Charles Bigras, and George Matzek* [2011] United States District Court for the Central District of California (September 2011).

account. This was done successfully using the funds withdrawal feature offered by OFSP 5 (see Figure 4).

Although the PayPal® account which was used to purchase virtual currency for Beneficiary 2's OFSP 5 account was initially set up without any problems, a number of weeks after the account's creation, and a number of successful transactions had been processed through the account, the PayPal® account was limited. While an account is limited the account holder can receive or request money, update account information, add a card, add a bank account and send refunds but the account holder cannot send money, withdraw money from the account, close the account, add money to the account, remove a card or remove a bank account. PayPal® sent an email to Beneficiary 2 asking for new credit card details and proof of address. They specifically asked for a utility bill, clearly showing the address of the account holder, and some form of government identification.

Coupled with the fact that OFSP 1 could not confirm the address supplied at the account opening stage, the account was limited by PayPal® because one or both of the transactions performed on the account were flagged as suspicious when the account was being routinely screened[25]. Although both payments were processed correctly at the time the transactions took place, PayPal® later put a 'temporary hold' on both transactions until a review was carried out. These transactions were subsequently refunded back to the prepaid Visa® gift card.

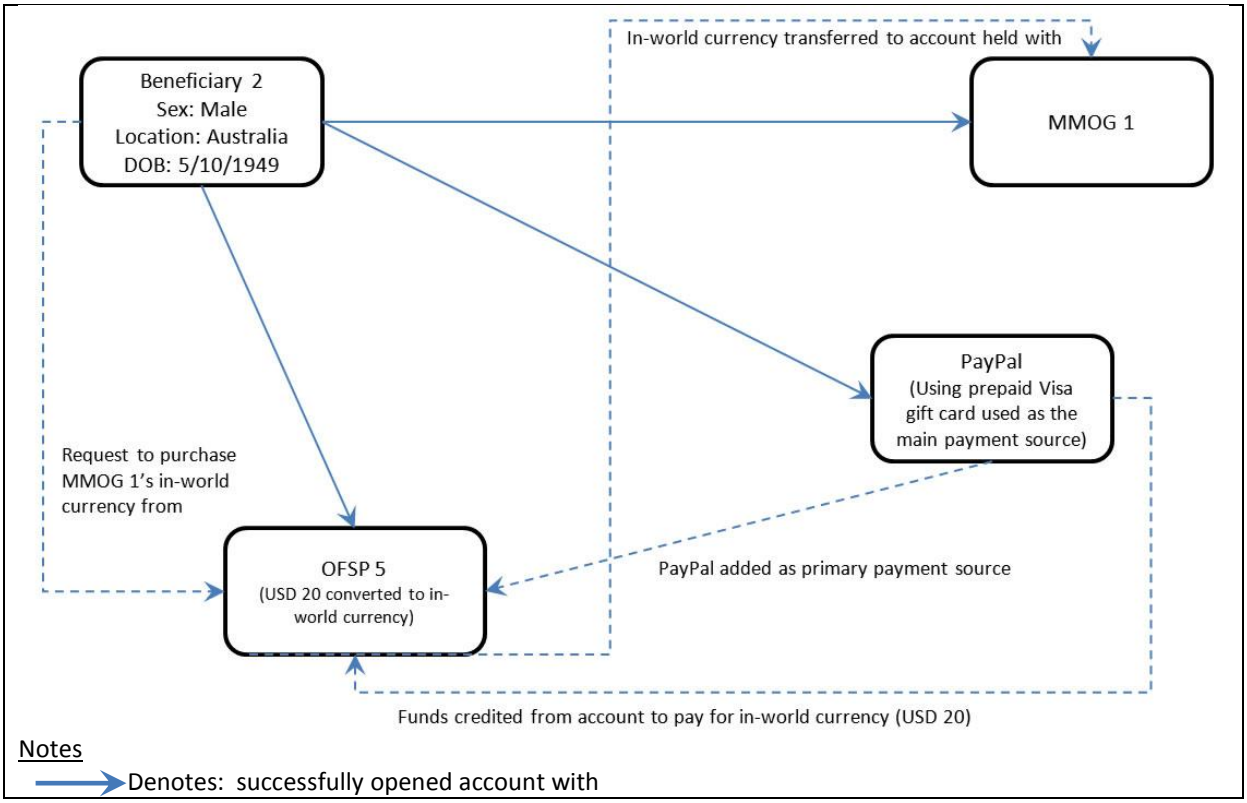

Figure 4: Successful in-world currency transfer from OFSP 5 to MMOG 1 using a prepaid Visa® gift card (Source: Authors)

Not only was the above-mentioned PayPal® account limited, it was discovered shortly after that all three[26]accounts set up with OFSP 5which utilised the suspect PayPal® account and/or attached prepaid Visa® gift card, had also been disabled. It appears thatPayPal® communicated to OFSP 5

[25] Reason provided by OFSP 1
[26] Third Party, Beneficiary 1 and Beneficiary 2

that a possible fraud had taken place and OFSP 5 took action to prevent any further activity through these accounts.

In contrast, both MMOG 2 and MMOG 3 accepted a PayPal® account with a prepaid Visa® gift card as the primary payment source when purchasing virtual currency.

The next set of experiments investigated whether any of the MMOGs who required a credit card to purchase virtual currency would accept a prepaid Visa® gift card as a valid payment method.

MMOG 1 would not accept a prepaid Visa® gift card in payment for their virtual currency. In contrast, both MMOG 2 and MMOG 3did accept a prepaid Visa® gift card as a valid credit card payment method. However, although funds were initially successfully added to the MMOG 2 account ofBeneficiary 2 using both the PayPal® and IcePay® pay by credit card methods, approximately two weeks after the transactions took place, the Beneficiary 2 avatar account was frozen by MMOG 2 because PayPal® had reversed the charges/taken the funds back and MMOG 2 themselves refunded the funds back to the prepaid Visa®gift card used to make the IcePay® purchase because the prepaid Visa® gift card was not a 3DS card. 3DS cards use Verified by Visa® or MasterCard® Secure Code as an additional security measure.

When it comes to placing funds into virtual environments using anonymous payment methods such as prepaid Visa®/MasterCard® gift cards, the results were mixed. Only MMOG 1's IVCES would not accept payment using prepaid Visa®/MasterCard® gift cards or PayPal® accounts utilising a prepaid Visa®/MasterCard® gift card, opting only to accept credit cards associated with a bank account. This measure goes some way to helping MMOG 1 to identify the individual who carried out the transaction, however, this task gets a lot more complicated when the card used to make the purchase is stolen or set up using a stolen or fictitious identity. MMOG 2 will accept a PayPal® account where the primary payment source is a prepaid Visa®/MasterCard® gift card. However, they will not directly accept a prepaid Visa®/MasterCard® gift card as a payment source.Only MMOG 3, allowed funds to be placed into accounts using both a prepaid Visa® gift card and a fictitious verified PayPal® account whose primary payment source is also a prepaid Visa® gift card. It is therefore possible to carry out transactions inside MMOG 2 and 3 which are untraceable, this is because these two service providers do not collect personally identifiable information from account holders when accountsare established; they do not collect billing information when transactionsare performed and transactions can be carried out either directly using prepaid Visa®/MasterCard®gift cards or indirectly using PayPal® accounts which draw on prepaid Visa®/MasterCard® gift cards as their payment source.

4.2 OFSPs

4.2.1 Personal information required from an account holder to set up an account

As can be seen from Table 4, OFSPs 1 and 2 required a substantial amount of personal information to set up an account. OFSPs 3 and 5 required no more than a valid email address to open an account. Although OFSP 4 did not have account setup procedures, they did required a little more in the way of personal information to place an order for virtual currency.

Only OFSPs 1, 2 and 4 collect information sufficient to establish the identity of account holders. The personal information collected by OFSPs 3 and 5 is wholly inadequate as the minimum information required to successfully verify an individual's identity is their full legal name and date of birth or residential address.

4.2.2 Identityverification procedures performed by OFSPs

The level of identity verification varies among the five OFSPs investigated (see Table 4). OFSPs 1, 2 and 4 claim to have the most stringent identity verification measures in place with each claiming to check the details provided by account holders against public record and requiring documented evidence from account holders, in the form of photo ID and utility bills, to prove that the account holder resides at the address used to set up the account. OFSPs 3 and 5, on the other hand, have fairly basic identity verification measures in place. The only verification measures they undertake is to send a verification link to the email address used to set up the account and record the IP address of the account holder.

The following paragraphs discuss in more detail the identity verification procedures implemented by each of the OFSPs under reviewand explore whether the current processes are sufficient to uncover the identities of those who may wish to use such environments to conduct money laundering and terrorism financing activities.

OFSP 1 initially checks the information provided by an account holder against public records. If the service provider is unable to verify the identity of the account holder against public records, they will send an email to the account holder requesting that he or she electronically send them certain documents as proof of identity. Until the identity has been confirmed, the service provider will not provide any services to the account holder, including withdrawing and receiving money. If an account holder provides a contact number that is unreachable, his or her account may be restricted.

OFSP 1 claimed to undertake the most stringent identity and payment method verification procedures. However, an account was successfully set up for Beneficiary 2 even though they were unable to verify the address provided against records held by Australia Post™ and the telephone number provided did not exist. No further identity verification was requested and the account was successfully setup and used to purchase virtual currency from OFSP 5. These funds were subsequently successfully transferred onwards to an avatar account held with MMOG 1. Although the account with OFSP 1 was initially set up without any problems, a number of weeks after the account's creation, and a number of successful transactions had been processed through the account, the account was limited. An email was sent to Beneficiary 2 asking for new credit card details and proof of address in the form of a utility bill and some form of government ID.

Although OFSP 2 requires a great deal of mandatory information to set up an account, it is extremely easy to open both personal and business accounts using bogus identity details and details of real-world businesses obtained from the Internet. For example, we were able to set up an account for Suspect 3 and open a business account for Business 2 in the name of a real-world business using publicly available information. A lot of information[27] was requested to open the business account, however, the company registration number was the only piece of information that would have proven difficult to obtain and may have highlighted to OFSP 2 that the account was fraudulent, but this was not a mandatory field.

On successfully creating an account with OFSP 2, account holders are automatically provided with an AUD 1,200 outgoing transaction limit and an AUD 1,500 per transaction limit. The outgoing transaction limit can be increased by verifying the account holder's Social Security Number, address or bank account. However, none of these verification methods were selected for the accounts created as it would be impossible for us to successfully verify them. In addition, it would be difficult

[27]Company name, registered country, legal form, registration number and address (not a PO box); business contact – title, name, position, work telephone number, mobile telephone number and date of birth; account details – currency, language, email address and password

for a would-be criminal to maintain anonymity by doing so. It should be noted that criminals could use straw men or third parties to set up and verify accounts in their own name and give the criminal exclusive access to these for a small fee or commission.

The outgoing and per transaction limit placed on an unverified account may prove to be insufficient for the purposes of large scale money laundering operation, however, if a number of these accounts were successfully opened, this could be an attractive method of getting funds to a terrorist organisation with little risk of being detected. Once the funds are inside the account, they can be transferred to any location around the world.

OFSP 3 provides the account holder with an access PIN number which they send to the email address provided by the account holder at account setup. Logging into the account using the PIN number verifies the account holder. OFSP 3 does not sell its currency directly to account holders; instead, it uses numerous digital currency exchanges to assist account holders to convert national currency into virtual currency and virtual currency back into national currency. OFSP 3 leaves the serious issue of identity and payment method verification to their exchange service providers.

There are no account setup procedures for OFSP 4. If a customer wishes to purchase virtual currency he or she must submit an electronic buy order form. Once the buy order form has been successfully submitted, the customer is issued with the service provider's bank account details. The customer deposits cash into OFSP 4's bank account and then must email information about the deposit[28] to OFSP 4. Failure to provide this information will result in the order being delayed. All first time orders with OFSP 4 are subject to telephone verification. As part of the verification process customers may also be required to provide a copy of their photo ID. For these reasons we were unable to place an order for virtual currency using the electronic buy order form. However, this method of submitting funds to an account may provide good levels of anonymity to a criminal, money launderer or terrorism financer, especially if they have access to false identity documents and an untraceable telephone number - all of which can be obtained over the Internet for a small charge (Winder, 2008 and Riley, 2011). It should be noted, however, that this method of payment can never be truly anonymous. This is because funds must be entered into OFSP 4's account using real-world financial institutions, which may have surveillance cameras in their premises and can be used to identify depositors.

Customers can also purchase a debit card from OFSP 4's, which is accepted at ATM machines around the world, and can be paid for and funded with virtual currency. To obtain a debit card, the customer must provide photo ID and a utility bill as proof of address. Again, we were unable to order or carry out any financial transactions using the debit card service offered by OFSP 4. This is because the cards would be posted to an address that did not exist and Beneficiary 2 would be required to go through telephone verification at the time of his first order. In addition, OFSP 4 would require photo ID and a utility bill as proof of identity and address.

OFSP 4 has very effective customer identity verification processes in place. Someone who wished to launder money would not use the debit card method to get funds into the financial system as there are too many ways that his or her true identity could be revealed. If a stolen identity (including postal address) was used to order the deposit card, the person might experience great difficulty retrieving the card from an address in which he or she is not a resident.

Similar to OFSP 3, OFSP 5 issues the account holder with a secret Terminal Identification Number (TIN). OFSP 5 sends an email containing instructions on how to activate the account to the email

[28] Including the name of the sender; the bank where the payment was made from (if a wire transfer); the date the payment was made; the exact amount the payment was for and the order reference number

address specified at account opening. The account must be activated within 24 hours of receiving the activation email or the account is cancelled. In order to transfer virtual currencies between an avatar account and the newly opened account, a link between the account and avatar must be established. After the link has been created the account holder must prove that he really owns the avatar by validating it at an in-world terminal owned by OFSP 5. Byvalidating an account, the account holder creates a permanent link between his or her avatar account and his or hernewly opened account, which is necessary for the effective and secure transfer of funds between accounts.

With some of the OFSPs investigated, the geographical location of an account holder may have some bearing on whether an account can be opened. For example, we attempted to open accounts for Third Party, who was purported to reside in Illinois, USA, with OFSP 2 and OFSP 5. The registration process could not be completed with OFSP 2 as the following message was displayed onscreen:

> "Due to legal restrictions, we cannot accept registrations from residents of Illinois. Please accept our apologies for this inconvenience".

However, OFSP 5 did not appear to be constrained by the same legal restrictions, as the account was opened successfully. OFSP 5 has no reliable way of identifying their account holders in a real-world context. Establishing a link between the OFSP 5 account and an Avatar account may have provided a useful source of information about the account holder, however, in many cases, no further information can be uncovered about the account holder from their Avatar account as, has been shown in the previous section, many MMOGs also do not collect sufficient information to identity their account holders.

The following conclusions can be drawn from the experiments conducted. Only OFSP 4 has effective customer identity verification processes in place. We were unable to perform any financial transactions with this service provider using our fictitious personas as this service provider required the account holder to provide documented proof of their identity and verification of their postal address before any transactions could be finalised. If a criminal, money launderer or terrorism financer wanted to achieve high levels of anonymity, they would not use OFSP 4 to get funds into the financial system as there are too many ways that his or her true identity could be revealed. All other OFSPs allowed us to open accounts and perform financial transactions using the fictitious identities, even though they claimed to verify an account holder's identity using a range of photo ID and official documents. Identity verification did not take place when the fictitious accounts were opened or after financial transactions had taken place. If the OFSPs had performed the identity verification procedures that they claimed to carry out at account opening, we would not have been successful in opening these accounts and performing financial transactions as we would not have been able to produce the documents necessary to verify the accounts.

Only OFSP 1picked up on anomalies with the information provided by the fictitious persona at the account opening phase but they did not act until after a number of financial transactions had taken place through the account. OFSP 1 should have acted on their first suspicion and disallowed any movement of funds through this account as it can be extremely difficult to trace the funds once they have been layered[29] through a number of different accounts, service providers and jurisdictions. Once funds cross jurisdictional borders, detection becomes more difficult due to the differing AML/CTF regulations and privacy implications and inconsistent levels of co-operation between AML/CTF and law enforcement agencies.

[29] Layering involves creating layers of transactions in an attempt to obfuscate the money trail.

Section ID		OFSP 1 Internet payment system	OFSP 2 Internet payment/fund transfer/ e-Wallet service	OFSP 3 Gold-based currency & payment solution provider	OFSP 4 Online virtual currency/ virtual gold exchange	OFSP 5 Virtual currency exchange
4.2.1	Personal information required from an account holder to set up an account and perform financial transactions with service provider:	• Email address • Name (full legal name) • DOB • Telephone number • Residential address (not a PO Box) • Confirmation of whether the account holder is a politically exposed person (PEP) or associated with someone who is (Tick box)	• Name • Country of residence • Address (not a PO Box) • Previous address (if lived at current address for less than 2 years) • Telephone number • Date of birth • Currency • Preferred language • Email address • Password	• Valid email address • Password	No account setup procedures. However, an electronic buy order form is used to collect the following information: • Virtual currency type • Virtual currency account number • Name on virtual currency account • First name • Last name • Email address • Home telephone (not a mobile) • Work telephone (not a mobile) • The amount of funds the customer wishes to purchase • Payment option	• Username • Email address • Avatar name • First name • Last name • Country (pre-selected) • Preferred language
4.2.2	Identity verification procedures:	• Verification email • Postal address verified against public record (in this experiment the address was verified against records held by Australia Post™) • Telephone number (sometimes used to verify the account holder)	• Verification of social security number • Verification of bank account • Verification of postal address	• PIN number sent to email address provided	• Customers may be required to provide a copy of photo ID • Photo ID, and utility bill must be provided when purchasing the service provider's debit card • Deposit card is sent by post to the contact address used to place the order	• Email containing information about how to activate account sent to specified email address
4.2.3	Payment method verification procedures:	Charges the bank account or credit card with a small charge. A reference number is also provided at this time. The reference number must be entered into the account holder's account profile.	The service provider charges the bank account or credit/debit card with a small random verification fee which must be entered into the account holder's account profile.	Carried out by individual virtual currency exchange services	All first orders are subject to telephone verification.	A link must be created between the account created and Avatar account
4.2.4	Payment methods accepted (for uploading funds):	Bank account, credit card	Credit card, bank transfer, Internet banking via POLi™	OFSP 3 does not sell its currency directly to account holders.	Virtual currency credits (available from Australia Post™), direct deposit[30], service provider debit card	Pay terminal inside MMOG, PayPal®, Bitcoin©, DIRECTebanking, PaySafeCard®, Moneybookers©, bank transfer
4.2.5	Other KYC/CDD, AML/CTF or anti-fraud measures in place:	None found	IP address recorded	IP address recorded every time the account holder logs into his or her account	None found	IP address recorded
4.2.6	Accept unverified payment methods?	Yes	Yes	No	Yes[31]	Yes

Table 4: Identity and payment method verification procedures carried out by the OFSPs under review

[30] Direct deposit of cash into the service provider's bank account is available in the following countries: Australia, Austria, Czech Republic, Indonesia, Israel, New Zealand and Taiwan

4.2.3 Payment method verification procedures enforced by OFSPs

OFSP 1 verifies an account holder's bank account or credit card by applying a small charge to the credit card or bank account. A 4-digit reference number is attached to the withdrawal, which must be entered into the account holder's account profile. Until the account has been verified, OFSP 1 restricts the amount of funds that can be sent to or withdrawn by the account holder.

Account holders of OFSP 2 are verified by adding a credit or debit card to their account details. This is the minimum level of verification required as, until this is done, the amount of funds which can be uploaded to the account is set at zero. Once a credit card has been added to the account, the card must go through a verification procedure. OFSP 2 charges the credit or debit card with a small random verification fee. The account holder must check their card statement for the exact transaction amount and enter it into the 'verify credit/debit card' section ontheiraccount profile. Upon successful verification, the verification fee is refunded back to the account holder'saccount and the account holder is informed of his or her transaction limits. To increase the outgoing transaction limit, the account holder must verify his or her name by providing details attached to a bank account. To increase the outgoing transaction limit further, the account holder must verify his or her postal address. To verify a postal address, a verification letter is sent by regular post to the address provided when the account holder registered his or her account. The letter contains a verification code which the account holder must enter back at OFSP 2's website.

As mentioned previously, OFSP 3 does not sell its currency directly to account holders, they use a number of virtual currency exchanges to assist account holders put value into their account.With OFSP 4 payment method verification takes place at the same time as identity verification, see section 4.2.2.

OFSP 5 validates the payment method by asking the account holder to create a link between the OFSP 5 account and his or her Avatar account. Once the link has been created the account holder must prove that he really owns the avatar by validating it at an in-world terminal owned by OFSP 5. Byvalidating an account, the account holder creates a permanent link between the avatar account and thenewly openedOFSP 5 account. Linking accounts is necessary for the effective and secure transfer of funds between accounts. Funds can be added to an account holder's OFSP 5 account at any of the in-world terminals that can be found in most major MMOGs.

Although over sixty transactions were conducted with the OFSPs under investigation, only four transactions were flagged as suspicious and the accounts subsequently frozen or limited. Due to the limited funds for carrying out this research, many of the transactions were for relatively small amounts – well under the transaction limits imposed by the MMOGs, OFSPs and payment types investigated. Many more transactions may have been flagged as suspicious had the transactions been for larger amounts, however, it should be noted that the funds often involved in terrorism financing activity involve small, innocuous amounts, similar to those used in these experiments.

Even though four accounts were frozen or limited, the worst thing that has happened is that the funds held in these accounts have been lost. The real identity of the account holder is still unknown to the OFSPs involved and this would hinder any attempts to prosecute the perpetrators for money laundering or terrorism financing offences. If these transactions had been performed in a real-world financial environment, where face-to-face interaction was necessary, the perpetrators might have been at higher risk of being detected and caught, especially if they were using stolen/fake identity documents to open accounts and/or perform transactions.

4.2.4 Payment methods accepted by OFSPs for uploading funds

As can be seen from Table 4,OFSP 1 accepts only a bank account and credit card details as payment options. OFSP 2 accepts credit card details, bank transfers and Internet banking via POLi™. OFSP 3 does not sell its currency directly to account holders; therefore, account holders must use the services of a virtual currency exchange to add fundsto their account. OFSP 4 allows account holders to add funds to their accounts using virtual currency credits[32],direct deposit[33]or the service provider's own debit card. OFSP 5 accepts the widest range of payment methods, including pay terminals inside MMOGs, PayPal®, Bitcoin©, DIRECTebanking, PaySafeCard®, Moneybookers©and bank transfer. The type of payment methods accepted by each of the OFSPs is important for account holder identification purposes as they may provide a possible avenue to discovering the real-world identity of an account holder, due to the types of information that may be disclosed about an account holder when a financial transaction is performed.

Table 5 shows the levels of anonymity afforded to the payment methods accepted by each of the OFSPs investigated.

Payment Method	Level of anonymity	
	High	Low
Bank account/bank transfer		√
Credit card		√
Internet banking via POLi™		√
Virtual currency credits		√
OFSP 4 debit card		√
Direct deposit	√	
Pay Terminal inside MMOG	√	
PayPal®	√	
PaySafeCard®[34]	-	-
Bitcoin©	√	
DIRECTebanking		√
Moneybookers©	√	

Table 5: Levels of anonymity afforded to payment methods offered by theOFSPs investigated

As shown in Table 5, direct deposit, pay terminal inside MMOG, PayPal®, Bitcoin© and Moneybookers© provide high levels of anonymity.

When using the direct deposit payment method, the service provider supplies the account holder with a reference number which is used to deposit cash directly into the service provider's bank account. Although high levels of anonymity can typically be achieved when cash is deposited, this is not always the case. For example, anonymity can be reduced when funds are entered into the service provider's account using real-world financial institutions as surveillance cameras are usually present[35].

[32] Virtual currency credits can be purchased from Australia Post™ outlets nationwide
[33] Cash is directly deposited into the OFSPs bank account
[34] PaySafeCard® is not available in Australia therefore this could not be tested.
[35]Surveillance cameras can be circumvented if the account holder used strawmen, or nominees to deposit funds

The virtual currency credit payment method also utilises the deposit of cash at Australia Post™ outlets. Although identification does not need to be shown to place cash onto the virtual currency deposit card, the customer must provide a contactable address and telephone number when ordering the card as the card will be posted to the address provided and the customer will undergo telephone verification at the time of their first order.

When using a Pay Terminal insidea MMOG, the account holder is given the option to pay using twoonline payment solution/fund transfer providers[36]. Theseonline payment solution/fund transfer providers do not have sufficient customer identity procedures in place to accurately identify their account holders and accept prepaid Visa®/MasterCard® gift cards as a primary payment source. The MMOG themselves also do not have sufficient procedures in place to accurately identity their account holders (see section 4.1.2).

PayPal® and Moneybookers©, both online payment solutions/fund transfer providers, offer high levels of anonymity because users can set up their account using false identity details and link a prepaid Visa® or MasterCard® gift card to their account. As mentioned previously, allowing a prepaid Visa® or MasterCard® gift card to be added to an account as a valid payment method results in the financial trail being lost as these cards can be purchased at millions of outlets worldwide using cash and without the need to show any form of identification.

Bitcoin© accounts can be set up with little or no identity verification. When verification is carried out, this can be easily circumvented. Account holders are not required to tie a bank account to their virtual currency account, with many digital currency exchangers allowing account holders to deposit large sums of cash directly into the currency exchanger's bank account. Once the virtual/digital gold is placed into the user's account, it can easily be transferred to another account, exchanged for real gold or withdrawn in the form of cash and transferred to a destination anywhere in the world where it becomes more difficult to trace.

Under normal operating conditions the other payment methods offer low levels of anonymity because they require account holders or users to supply their credit card, bank account details or photo ID and utility bill as proof of address. The only way that the level of anonymity of these payment methods could be increased is if they allowed either a prepaid Visa® or MasterCard® gift card to be added as a valid payment method or stolen credit card details were used to set up the account or carry out the transaction. Section 4.2.6 investigates the use of prepaid Visa® gift cards to set up accounts and/or carry out anonymous transactions in greater detail.

4.2.5 Other KYC/CDD, AML/CTF or anti-fraud measures in place by OFSPs

OFSPs 2and 5 record the IP address of the account holderwhen setting up an account and OFSP 3 records the IP address of the account holder every time he or she logs into his or her account. However, as mentioned earlier, IP addresses can be successfully concealed using privacy enhancing software such as Tor Browser software, and, therefore, cannot be relied upon to reliably verify the account holder's identity or location.

No other KYC/CDD, anti-money laundering or anti-fraud measures were discovered during ourOFSPreview and experimentation phases.

[36] PayPal® and Moneybookers©

4.2.6 Can anonymity of a payment method accepted by an OFSP be increased by utilising a prepaid Visa®/MasterCard® gift card as a payment source?

A number of experiments were carried out to determine whether some of the payment methods classified as offering low levels of anonymity (see Table 5) could be increased to offer higher levels of anonymity by attaching a prepaid Visa® gift card as their payment source. These experiments were conducted using both the fictitious personas and the accounts set up with theMMOGs and OFSPs.

Experimentation found that a bank account/bank transfer, Internet banking via POLi™ and DIRECTebanking cannot utilise a prepaid Visa®/MasterCard® gift card as a payment source as the funds must come from a user's bank account. However, similar to that experienced with the MMOGs investigated, OFSPs 1 and 2 allowed us to use a prepaid Visa® gift card as a valid credit card payment. It is therefore possible to carry out transactions inside OFSPs 1 and 2 which are untraceable.

5. The feasibility of introducing KYC/CDD legislation into virtual environments

It is clear from our research that all of the MMOGs and most of the OFSPs investigated do not have systems in place that are able to accuratelyidentify, verify and authenticate the identity of their account holders or users. If MMOGs and OFSPs were to be used for illicit purposes, there would be no reliable way for the MMOG or OFSP operator or law enforcement, to identify and prosecute the perpetrator(s).

Brown (2010) investigates financial transactions inside virtual environments and makes a number of recommendations as to how vulnerabilities associated with customer identification can be combatted, namely, the introduction of regulation which would see Internet cafes and public spaces require that their customers show identification in order to document who is using their computers; users being mandated to prove their identity when converting virtual funds into real-world currency; implementation of bank licensing regulations to financial transactions which allow users to transfer virtual currency into real-world currency and the introduction of a compliance department, which should oversee virtual transactions within any virtual world medium. Brown (2010) believes, however, that the most reliable way to stop the potential for terrorism financing within virtual environments is to eliminate the ability for a user to exchange virtual currency into real-world currency. However, we believe that these solutions would be ineffective or heavy handed for the following reasons:

Introducing regulation which forces Internet cafe and public computer users to show identification would not eliminate money laundering and terrorism financing activity, it would only relocate the problem by forcing perpetrators to use privacy enhancing tools and software on their own personal computers, where it would be more difficult to detect.

The introduction of legislation which mandates users prove their identity when converting virtual currency into real-world currency would not be as straight-forward to police in virtual or online environments as they would be in traditional real-world financial environments due to the removal of face-to-face contact. It may be extremely difficult to detect when false identity documents are being used to set up an online account or perform financial transactions. In the real-world, if a customer wishes to open a new account, he is required to produce photographic ID and proof of his or her residential address. The teller would notice if the ID shown did not match the physical appearance of the person opening the account. When an account is opened online, the service provider cannot check the photographic ID provided against the appearance of the individual who is

opening the account. If an individual is verified online using paper or electronic documents, these can be easily doctored or forged using one of a number of inexpensive, readily available software tools. These doctored or forged documents can be of sufficient quality that they could go undetected by the untrained eye. In addition, much of money laundering and terrorism financing detection relies heavily on the physical cues picked up by financial institutions and reporting entities from depositors when they attempt to open or place funds into an account. These cues may include, defensive stance to questioning, attempts to conceal the origin and destination of cash transactions, refusal of the suspect to provide information about the true economic beneficiary of the funds. The removal of face-to-face contact removes an important method of detection.

The implementation of bank licensing regulations and the introduction of a compliance department maybe cost prohibitive for many MMOGs and OFSPs as they do not generate the income enjoyed by the banking sector. Many MMOGs and OFSPs are small, operate with minimal staff and charge a small fee for their service, therefore, may have insufficient income to put into place and enforce banking-type regulations. If legislation is to be put in place, it should take into account the unique operating environment and challenges faced by these organisations to ensure that there is a realistic outcome of compliance.

Inits current format,Australia's AML/CTF regulation does not appear to sufficiently deal with transactions which encompass virtual currency used in MMOGs. It is recommended that the definition of a designated service be broadened to include organisations which buy, sell and trade virtual currency used in MMOGs for real-world currency. Funds can be deposited into virtual environments using online currency exchanges, electronic funds transfers, remittance service/money transfer providers, stored value cards and bullion dealers. Although these designated services are currently covered under current KYC and CDD regulations, these regulations apply mainly to physical currency/money rather than virtualcurrency. For example, the AML/CTF Act states that currency exchange involves the 'physical' exchange of money/currency[37] which most commonly occurs at bureaux de changes, banks, hotels and airports within a retail environment. Physical currency/money, defined in section 5 of the AML/CTF Act, refers to coins and printed money which are designated as legal tender and circulates as, and is customarily used and accepted as, a medium of exchange in the country of issue. Although virtual currencies have a strong similarity to physical currency/money, i.e. they are interchangeable with real money and can be used to buy and sell goods and services inside virtual environments; they are not considered legal tender in the real world as they can be lawfully refused as payment. Even though virtual currency is not contractually backed by tangible assets or by legal tender laws, and is not a tangible commodity itself, for the purposes of AML/CTF legislation, the definition of money should be amended to include intangible, virtual funds.

We suggest that any regulations imposed on virtual environment operators should resemble those imposed on the online gambling industry as virtual environment operators' face the same challenges as online gambling firms when identifying, verifying and authenticating gamers (Levi, 2009).

[37] Under section 5 of the AML/CTF Act, money is defined as (a) physical currency; and (b) money held in an account, whether denominated in Australian currency or any other currency; and (c) money held on deposit, whether denominated in Australian currency or any other currency; and (d) e-currency, however amounts of the e-currency are expressed. Under section 5 of the AML/CTF Act, e-currency is defined as an internet-based, electronic means of exchange that is:(a) known as any of the following: (i) e-currency; (ii) e-money; (iii) digital currency; (iv) a name specified in the AML/CTF Rules; and (b) backed either directly or indirectly by: (i) precious metal; or (ii) bullion; or (iii) a thing of a kindprescribed by the AML/CTF Rules; and (c) not issued by or under the authority of a government body; and includes anything that, under the regulations, is taken to be e-currency for the purposes of the Act.

Gambling operators are obliged to reasonably identify the location and identity of account holders before allowing financial transactions to take place butKYC and CDD regulations do not mandate that every potential customer be required to produce irrefutable evidence of their identity before being allowed onto an online gambling website. Substantial documentation must be provided before any significant payments are made to the registered player.

MMOGs should be responsible for identifying, verifying and authenticating their own account holders even when financial transactions are performed via a third party OFSP. Performing identity, verification and authentication checks on every account holder would be cost prohibitive, especially when large numbers of account holders open accounts who have no intentions of ever performing financial transactions through these accounts. Therefore, checks should only be performed when the account holder transfers virtual or real funds out of their account(s). This enables account holders to place funds into their account to pay for membership fees and buy virtual goods and services without the need to go through extensive KYC and CDD procedures. Ongoing CDD should be performed as the relationship with the customer develops.

Rather than requiring extensive documentary evidence to verify an account holder's identity, we believe that the following electronic KYC approach (see Figure 5 for one such example) would be more suitable for identifying, verifying and authenticating MMOG and OFSP account holders/users.

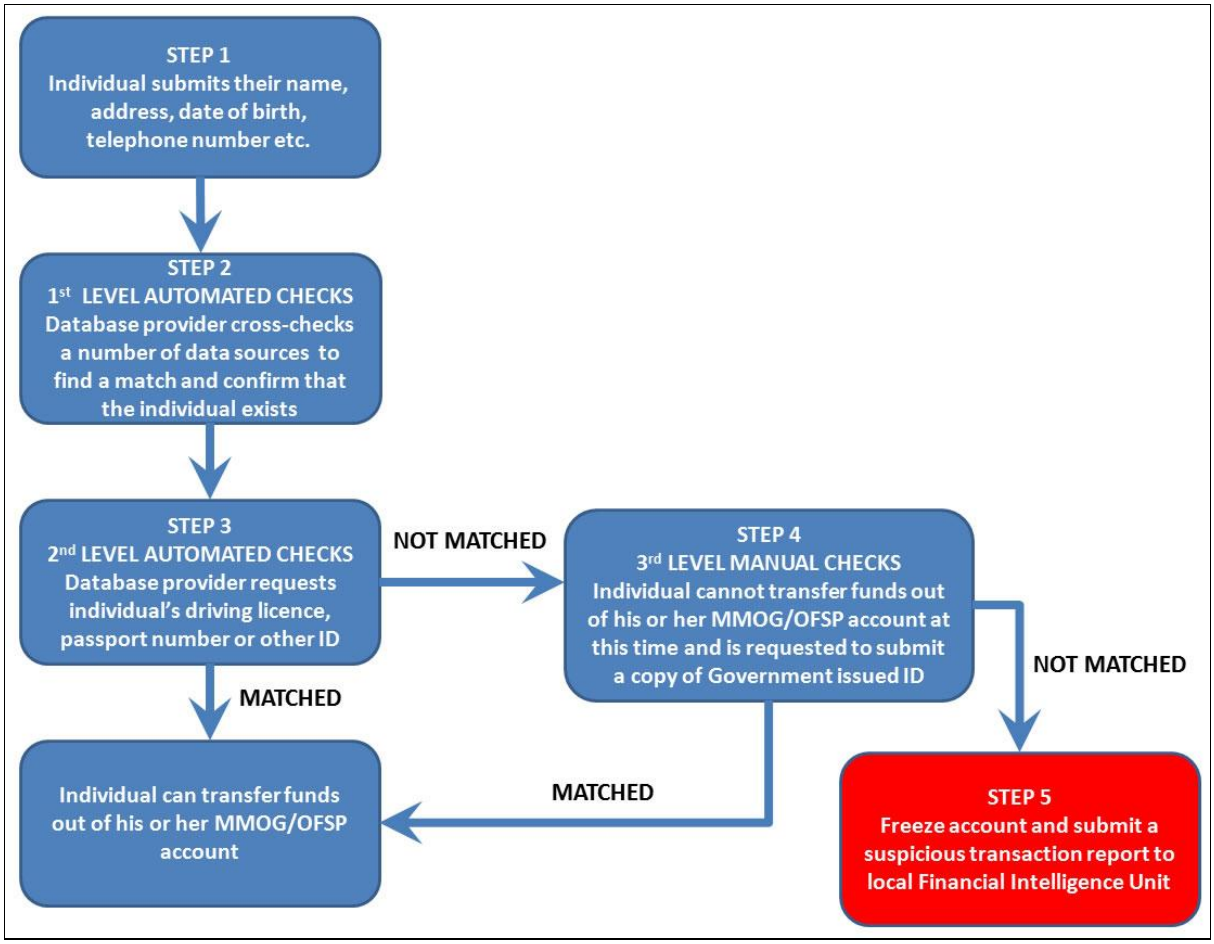

Figure 5: Example of electronic KYC approach (Source: Authors)

The first step of the electronic verification and authentication procedure would involve collecting the name, address, date of birth, and telephone number from the account holder. Step two would involve using a third party database provider to check the information provided by the account

holder against the records held by at least two electronic data sources. These data sources may include the Australian Electoral Roll, Sensis White Pages, GDC National Telephone File, GDC Citizen File and the Transaction History Database. Once the database provider is satisfied that the information provided by the account holder is correct and that the account holder does exist, the database provider would request the account holder's driving licence, passport number or other ID. If the information provided by the account holder matched that shown on the driving licence, passport or other ID, the account holderwould be allowed to make a funds transfer. If the information did not match, the account holder would be required to go through manual checking and requested to submit a copy of Government issued ID. If this information matched that provided by the account holder, the account holder would be free to make a funds transfer. However, if the information did not match, the account would be frozen and a suspicious transaction report submitted to the Financial Intelligence Unit in the MMOG or OFSPs local jurisdiction.

Using this electronic verification and authentication procedure would be more cost effective and reliable than traditional verification and authentication procedures as most genuine account holders would be successfully verified before manual checking was necessary and the challenges of identifying forged or doctored documentation would be removed.

We believe that it is unnecessary to eliminate the ability for users to exchange virtual currency into real-world currency as we believe that proper identification of account holders, such as that shown above, would go some way to reducing the attractiveness of virtual environments as a tool for money laundering and terrorism financing activity.

6. Conclusions

The most crucial aspect of any successful AML/CTF investigation is being able to identify the individuals involved and the transactions that they have carried out. However, the task of identifying individuals who use virtual and online environments to carry out such activities is extremely difficult, especially when KYC and CDD procedures are not fully implemented by the service provider; the individual deliberately attempts to conceal their identity using stolen or false identity documents and privacy enhancing software is used to conceal the user's IP address, thereby preventing service providers and law enforcement agencies from tracking their movements and activities.

Although OFSPs are already subject to AML/CTF regulations, in Australia and many other countries, these regulations relate to transactions involving 'real money', therefore, clarity or new regulation should be introduced which deals specifically with the purchase, sale and exchange of virtual currency used in MMOGs for real-world currency. In contrast, financial transactions which occur inside MMOGs are currently unregulated, therefore, it is recommended that new regulations be introduced which apply to the sale or exchange of virtual currencies which take place inside virtual environment and between third party financial service providers. These regulations should take into account the unique operating environment faced by virtual environment operators and their financial intermediaries. Unless appropriate regulations are introduced, which OFSPs and MMOGs can be held truly accountable, these organisations will have little incentive to put into place adequate KYC and CDD processes and procedures which successfully identity those that open accounts.

If AML/CTF regulations were introduced which dealt with transactions that take place inside and through virtual environments using virtual currency, virtual environment operators would be required by law to carry out appropriate identity verification procedures. We believe that the electronic KYC approach discussed in this paper deals effectively with the challenges of global reach,

anonymity and non-face-to-face business relationships experienced by virtual environment operators. Information supplied by account holderswould be verified by a reliable and independent source, thereby ensuring that effective CDD activities could be carried out.

References

ALRC (2011) Use and disclosure of credit reporting information: identity verification [www document] http://www.alrc.gov.au/publications/57.%20Use%20and%20Disclosure%20of%20Credit%20Reporting%20Information/identity-verification#_ftn131 (accessed: 24 November 2011)

Attorney General's Department (2012) Anti-Money Laundering and Counter-Terrorism Financing Act 2006 [www document] http://www.comlaw.gov.au/Details/C2012C00295 (accessed 28 March 2012)

AUSTRAC (2009) Introduction to Terrorism Financing [www document] http://www.austrac.gov.au/elearning/mod5/mod_5_terrorism_financing_8.html (accessed: 15 October 2011)

AUSTRAC (2012[A]) Introduction to Money Laundering [www document] http://www.austrac.gov.au/elearning/pdf/intro_amlctf_money_laundering.pdf) (accessed: 7 March 2012)

AUSTRAC (2012[B]) Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No.1) [www document] http://www.comlaw.gov.au/Details/F2012C00099/Download (accessed: 7 March 2012)

British Broadcasting Corporation News (2008) Poor earning virtual gaming gold, 22 August 2008 [www document] http://news.bbc.co.uk/2/hi/7575902.stm (accessed: 20 February 2012)

Brown, H A (2010) Virtual Worlds – A tool for money laundering and terrorist financing? ACAMS Today, March – May 2010

Choo, K-K R (2008[A]) Money laundering and terrorism financing: Risks of Prepaid Cards/Instruments, Asian Journal of Criminology, Volume 4, Number 1

Choo, K-K R (2008[b]) Organised crime groups in cyberspace: a typology, Trends in Organized Crime, Volume 11, Issue 3, pp 270-295

Choo, K-K R & Smith, R G (2008) Criminal Exploitation of Online Systems by Organised Crime Groups, Springer Science, Asian Criminology, Volume 3, pp 37 – 59

FATF-GAFI (2012) International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation - The FATF Recommendations [www document] http://www.fatf-gafi.org/dataoecd/49/29/49684543.pdf (accessed: 28 March 2012)

FATF-GAFI.org (2011) How is money laundered? [www document] http://www.fatf-gafi.org/document/29/0,3746,en_32250379_32235720_33659613_1_1_1_1,00.html (accessed: 23 March 2012)

FBI (2008) Department of Justice launches new law enforcement strategy to combat increasing threat of international organized crime [www document] http://www.justice.gov/opa/pr/2008/April/08-opa-330.html (accessed: 16 March 2012)

Financial Supervision Commission (2009) Money laundering and the Financing of Terrorism [www document] http://www.fsc.gov.im/aml/ (accessed: 20 February 2012)

Financial Transactions and Reports Analysis Centre of Canada (2009) Terrorist Financing [www document] http://www.fintrac.gc.ca/multimedia/education/c1/1-5-eng.asp (accessed: 9 October 2011)

Hardouin, P (2009) Banks governance and public-private partnership in preventing and confronting organized crime, corruption and terrorism financing, Journal of Financial Crime, Volume 16, Issue 3

Heeks, R (2008) Current analysis and future research agenda on "gold farming": real-world production in developing countries for the virtual economies of online games, Centre for Development Informatics, University of Manchester, United Kingdom [www document] http://www.sed.manchester.ac.uk/idpm/research/publications/wp/di/documents/di_wp32.pdf (accessed: 20 February 2012)

Irwin, A S M; Choo K-K R & Liu, L (2012[A]) An analysis of money laundering and terrorism financing typologies, Journal of Money Laundering Control, Issue 15:1

Irwin, A S M; Choo K-K R & Liu, L (2012[B]) Modelling of money laundering and terrorism financing typologies, Journal of Money Laundering Control, Issue 15:3

Leapman, B (2007) Second Life® world may be haven for terrorists [www document] http://www.telegraph.co.uk/news/uknews/1551423/Second-Life-world-may-be-haven-for-terrorists.html (accessed: 20 February 2012)

Lee, J (2005) Wage slaves, Computer Gaming World, July/August, 20-23 [www document] http://www.1up.com/do/feature?cId=3141815 (accessed: 20 October 2011)

Levi, M (2009) Money laundering risks and e-gaming; a European overview and assessment [www document] http://www.egba.eu/pdf/Levi_Final_Money_Laundering_Risks_egaming%20280909.pdf (accessed: 20 February 2012)

Methenitis, M (2009) Virtual world money laundering, Law of the Game, 3 June 2009 [www document] http://lawofthegame.blogspot.com/2009/06/virtual-world-money laundering.html (accessed: 23 February 2012)

Nardo, M (2006) Building synergies between theory and practice: Countering financial crime on a systemic approach, Journal of Financial Crime, Volume 13, Issue 3

Palmer, C (2005) A picture of terrorist financing, Counter Terrorist Financing, AML Newsletter, December 2005 [www document] http://www.amlmagazine.com.au/amlwr/_assets/main/lib7006/a%20picture%20of%20terrorist%20financing_issue2_december05.pdf (accessed: 3 June 2011)

Rijock, K (2007) China's central bank will regulate virtual currency, 13 January 2007 [www document] http://www.world-check.com/articles/2007/01/13/chinas-central-bank-will-regulate-virtual-currency/ (accessed: 15 February 2012)

Riley, M (2011) Stolen credit cards go for $3.50 @ Amazon-like online bazaar [www document] http://www.bloomberg.com/news/2011-12-20/stolen-credit-cards-go-for-3-50-each-at-online-bazaar-that-mimics-amazon.html (accessed: 24 April 2012).

Sanders, M (2009) Money laundering through gold framing and virtual goods, 3 June 2009 [www document] http://www.box.net/shared/nikjjgng3m (accessed: 15 February 2012)

Sullivan, K (2008) Virtual money laundering and fraud: Second Life® and other online sites targeted by criminals, 3 April 2008 [www document] http://www.bankinfosecurity.com/articles.php?art_id=809 (accessed: 15 February 2011)

Tefft, B (2007) Will 5 new unregulated virtual banks become money laundering centres? 12 January 2007 [www document] http://www.world-check.com/articles/2007/01/11/will-5-new-unregulated-virtual-banks-become-money-/ (accessed: 15 February 2012)

Winder, D (2008) Stolen Australian credit cards going cheap [www document] http://www.itwire.com/your-it-news/home-it/21099-stolen-australian-credit-cards-going-cheap (accessed: 24 April 2012)

WorldBank.org (2003) Money laundering and Terrorist Financing: Definitions and Explanations, Chapter 1, 30 March 2003 [www document] http://www1.worldbank.org/finance/assets/images/01-chap01-f.qxd.pdf (accessed: 25 March 2012)