Uniting Church in Australia
SYNOD OF VICTORIA AND TASMANIA

Justice and International Mission Unit
130 Little Collins Street
Melbourne Victoria 3000
Telephone: (03) 9251 5271
Facsimile: (03) 9251 5241
jim@victas.uca.org.au

8 September 2017

Committee Secretary
Senate Legal and Constitutional Affairs Committee
PO Box 6100
Parliament House
Canberra, ACT 2600
E-mail: legcon.sen@aph.gov.au

Submission of the Synod of Victoria and Tasmania, Uniting Church in Australia on *Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2017*

The Synod of Victoria and Tasmania, Uniting Church in Australia, welcomes the opportunity to provide a submission on the *Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2017*.

Digital Currencies

The Synod strongly supports the inclusion of digital currency exchange providers under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006.* At the 2016 meeting of approximately 400 representatives of the Synod from across Victoria and Tasmania the following resolution was adopted:

> *The Synod resolved:*
> *(a) To affirm that virtual currencies have legitimate uses in reducing online transaction costs and speeding up some online transactions, and that the appropriate response to their misuse is to bring them under regulation that already applies to normal currencies to prevent the virtual currencies being used in harmful transactions;*
> *(b) To join with the Senate Economics Reference Committee and the Productivity Commission in calling for virtual currencies to be brought under regulation through the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 so those providing virtual currency services that are operating like banks and other financial institutions are required to take reasonable steps to prevent virtual currencies being used to harm people. Such steps should include requirements to know their customers, to keep records of transactions, to report suspicious transactions to law enforcement agencies and to refuse to carry out transactions where they believe there is a high likelihood the transaction involves criminal activity; and*
> *(c) To write to the Minister of Justice and the Shadow Minister of Justice to inform them of this resolution.*

Those providing virtual currency services that are operating like financial institutions should be required to take reasonable steps to prevent virtual currencies being used for criminal activities, such as tax evasion and the purchase of child sexual abuse material. Such steps should include requirements to know their customers, to keep records of transactions, to report suspicious transactions to AUSTRAC and to refuse to carry out transactions where they believe there is a high likelihood the transaction involves criminal activity. The FATF has argued that transaction monitoring and suspicious activity reporting are essential for such providers.[1]

[1] FATF, 'Guidance for a Risk-Based Approach. Prepaid Cards, Mobile Payments and Internet-Based Payment Services', June 2013, 22.

The Synod agrees with the provisions of the Bill to require digital currency exchange providers to:

- Enrol and register on a Digital Currency Exchange Register maintained by AUSTRAC and provide prescribed registration details;
- Adopt and maintain an AML/CTF program to identify, mitigate and manage money laundering and terrorism financing risks they may face;
- Identify and verify the identities of their customers;
- Report suspicious matters to AUSTRAC; and
- Keep certain records related to transactions, customer identification and their AML/CTF program for seven years.

However, the Synod also believes there should be an explicit requirement that digital currency exchange providers refuse to carry out transactions that have a high likelihood of being associated with criminal activity, unless instructed to carry out the transaction by a law enforcement agency that wishes to avoid the criminals being tipped off by the refusal to carry out the transaction.

The Synod supports Section 76G which enables the AUSTRAC CEO to impose conditions on the registration of a person as a digital currency exchange provider. The Synod supports that these conditions may relate to (without limitation):

- The value of digital currency or money exchanged;
- The volume of digital currency being exchanged (whether by reference to a particular period, a particular kind of digital currency, or otherwise);
- The kinds of digital currencies exchanged; and/or
- Requiring notification of exchange of particular kinds of digital currency, changes in circumstances or other specified events.

The Synod supports paragraph 76H(1)(c) to ensure that the registration of a digital currency exchange provider must be renewed every three years.

In March 2013, the Financial Crimes Enforcement Network (FinCEN) issued guidance applying anti-money laundering and counter terrorism financing (AML/CFT) rules to digital economy exchanges. The guidance explains that under the revised money service businesses (MSBs) rule, exchangers and administrators of convertible virtual currency are regulated as money transmitters. They must also file Suspicious Activity Reports on suspicious transactions.[2]

In June 2013 the FATF recommended that providers of new payment products and services, including digital and virtual currencies, that fall within the definition of financial institution by conducting money or value transfer services, or by issuing and managing a means of payment, should be subject to Anti-Money Laundering/Counter Financing Terrorism preventative measures as required by the *FATF Recommendations*. This includes customer due diligence, record keeping and reporting of suspicious transactions.[3] The FATF argues that transaction and customer due diligence records are key to AML/CFT efforts and support law enforcement investigations. At a minimum**,** the transaction record of a payment or funds transfer should include information identifying the parties to the transaction, any account(s) involved, the nature and date of the transaction, and the amount transferred. The records that are retained should be sufficient to allow the tracing of funds through the reconstruction of transactions.[4]

Digital currencies are not just used for money laundering, but to facilitate criminal activities that require anonymity. Appendix 1 provides some examples of the misuse of digital currencies for criminal purposes.

[2] International Centre for Missing & Exploited Children and Thomas Reuters, 'The Digital Economy: Potential, Perils and Promises. A Report of the Digital Economy Task Force', March 2014, 17.
[3] FATF, 'Guidance for a Risk-Based Approach. Prepaid Cards, Mobile Payments and Internet-Based Payment Services', June 2013, 12.
[4] FATF, 'Guidance for a Risk-Based Approach. Prepaid Cards, Mobile Payments and Internet-Based Payment Services', June 2013, 24.

Daniel Mossop, director of financial crime in the Attorney-General's Department in 2015, said that Australian law enforcement agencies had limited oversight of digital currencies:[5]

> *We don't have eyes on bitcoin being transferred between people. We would see it if it came out of an offramp (if s converted into standard currency), but as it gets more mainstream and more people accept it, there won't be a need for it to come out an offramp or out of the bitcoin system.*

AUSTRAC's internal assessment of the money laundering risks associated with Bitcoin has been:[6]

> *Yet Bitcoin is also vulnerable to money laundering as a result of the mechanisms through which it operates on such as:*
> *• The ability to open a bitcoin wallet (or account) and transfer value with no customer due diligence or identification.*
> *• The ability to disguise movement of value by changing it into different types of mainstream currency.*
> *• Poor visibility of transaction history*
> *• Movement of large amounts of funds between individuals and accounts offshore without limits on value*
>
> *Criminals accepting payment for Bitcoins for illicit goods and services do not need to place physical cash within the financial system. This step is bypassed by accepting bitcoins directly instead of cash.*

The FATF recommends that countries should require the licensing or registration of providers of money or value transfer services, and they should take action to identify natural or legal persons that carry out money or value transfer services without such a licence or registration.[7] Further, to assist in the supervision of services provided in their jurisdiction, the FATF states that countries could consider, consistent with their legal frameworks, prohibiting Internet-based payment services from offering services in their jurisdiction without a physical presence, in the form of a local office or agent, in that jurisdiction.[8]

The US Treasury Department has stated that the exchange of virtual currencies for fiat currencies opens the door to regulation through current laws for "money service businesses".[9] The US requires all providers of money and value transfer services, wherever they may be based in the world, to be licensed and registered in the US if the money or value transfer service offers services in the US.[10]

Allowing Related Bodies to Share Information

The Synod supports related businesses being able to share due diligence and suspicious mater reports to increase the effectiveness of the anti-money laundering and counter-terrorism financing regime. Requiring related businesses to have to perform due diligence on the same person multiple times increases the likelihood a person involved in money laundering or terrorism financing will slip through undetected and increases the costs on businesses as different parts of the same related business have to carry out due diligence separately. For the same reason, the Synod would be open to unrelated businesses being able to share due diligence and suspicious

[5] Jessica Sier, 'Rush to regulate bitcoin as 'mum and dads' use it to buy drugs', *The Australian Financial Review,* 4 March 2015, http://www.afr.com/technology/web/ecommerce/rush-to-regulate-bitcoin-as-mums-and-dads-use-it-to-buy-drugs-20150304-13v2ta

[6] AUSTRAC, 'Criminal usage of Bitcoin. Operational Intelligence Report', 2, http://www.austrac.gov.au/sites/default/files/1617-095-document-for-release-6026272.pdf

[7] FATF, 'Guidance for a Risk-Based Approach. Prepaid Cards, Mobile Payments and Internet-Based Payment Services', June 2013, 32.

[8] FATF, 'Guidance for a Risk-Based Approach. Prepaid Cards, Mobile Payments and Internet-Based Payment Services', June 2013, 32-33.

[9] International Centre for Missing & Exploited Children and Thomas Reuters, 'The Digital Economy: Potential, Perils and Promises. A Report of the Digital Economy Task Force', March 2014, 14.

[10] FATF, 'Guidance for a Risk-Based Approach. Prepaid Cards, Mobile Payments and Internet-Based Payment Services', June 2013, 44.

matter reports with safeguards to protect any unnecessary intrusion on privacy and minimising the risk of tipping off someone involved in money laundering or financing terrorism that they have been detected. It is our view that the anti-money laundering and counter-terrorism financing system would be more robust if the ability of those attempting to launder money or finance terrorism had less chances to try multiple entry points to get the money into the system because there was better sharing of information between reporting entities.

Increased Powers for AUSTRAC

The Synod supports the Bill's provisions to strengthen AUSTRAC's investigation and enforcement powers by:

- Giving the AUSTRAC CEO the power to issue infringement notices for a greater range of regulatory offences; and
- Allowing the AUSTRAC CEO to issue a remedial direction to a reporting entity to retrospectively comply with an obligation that had been breached.

The Synod supports the provision of additional powers to issue infringement notices by the AUSTRAC CEO to increase the enforcement options that AUSTRAC has at its disposal to encourage compliance by reporting entities with their AML/CTF obligations. The penalty level of the infringement notice at 60 penalty units for a body corporate will represent a fairly minor financial cost on many reporting entities, justifying that such a penalty should be able to be imposed without the involvement of the courts and leaving court action for more serious violations of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006.*

Review of criminological literature on what works to deter crime finds that perceived certainty of punishment is associated with reduced intended offending.[11] The conclusion is that certainty of apprehension and not the severity of the legal consequences ensuing from apprehension is the more effective deterrent.[12]

Recent meta-analysis of what works to deter businesses breaking the law found that a combination of enforcement strategies worked best, rather than the over reliance on just one strategy.[13] A combination of law, regulatory policy and punitive sanctions was found to have a significant deterrent effect on businesses breaking the law. Inspections had the greatest deterrent effect on businesses willing to break the law.[14] The researchers concluded:

> *….it makes sense to focus on regulatory policies at the middle level of the [regulatory] pyramid where persuasion is generally most needed to achieve compliance. Specifically, our findings indicate that policies may be more successful when industry has some input and policies are coupled with education and consistent inspections. More severe strategies (regulatory investigations, penalties, civil suits and arrest/jail time) should be added where compliance has been difficult to achieve.*[15]

Further:[16]

> *Results offer support for a model of corporate regulatory enforcement that blends cooperation with punishment –the type and amount of enforcement response to be determined by the behaviour of the manager/ company (i.e., responsive regulation). Thus, at the top and even*

[11] Daniel S Nagin, 'Deterrence in the Twenty-First Century', *Crime and Justice* Vol. 42, No. 1, (August 2013), 201.
[12] Daniel S Nagin, 'Deterrence in the Twenty-First Century', *Crime and Justice* Vol. 42, No. 1, (August 2013), 202.
[13] Natalie Schell-Busey, Sally Simpson, Melissa Rorie and Mariel Alper, 'What Works? A Systematic Review of Corporate Crime Deterrence', *Criminology and Public Policy* Vol. 15 No. 2, (2016), 401.
[14] Natalie Schell-Busey, Sally Simpson, Melissa Rorie and Mariel Alper, 'What Works? A Systematic Review of Corporate Crime Deterrence', *Criminology and Public Policy* Vol. 15 No. 2, (2016), 404.
[15] Natalie Schell-Busey, Sally Simpson, Melissa Rorie and Mariel Alper, 'What Works? A Systematic Review of Corporate Crime Deterrence', *Criminology and Public Policy* Vol. 15 No. 2, (2016), 406.
[16] Natalie Schell-Busey, Sally Simpson, Melissa Rorie and Mariel Alper, 'What Works? A Systematic Review of Corporate Crime Deterrence', *Criminology and Public Policy* Vol. 15 No. 2, (2016), 408.

middle levels of the enforcement pyramid, multiple "levers" may need to be pulled to achieve compliance.

Put simply, giving a law enforcement body more options in leveraging compliance allows them greater flexibility to apply a proportionate response to obtain compliance.

Bearer Negotiable Instruments

The Synod supports the provisions in the Bill giving police and customs officers broader powers to search and seize physical currency and bearer negotiable instruments (BNI) and establish civil penalties for failing to comply with questioning and search powers.

Bearer share warrants are a vehicle to facilitate money laundering. As an example, in the case of Syed Ziaddin Ali Akbar, who was the former head of the BCCI Central Treasury from 1982 to 1986 and was charged and convicted in October 1988 of laundering drug money at UK Trading House.[17] In an attempt to defeat asset recovery efforts by law enforcement, in January 1989 he used bearer shares in a Vanuatu company to transfer assets to his brother.

Remittance Providers

The Synod is supportive of the amendment to section 75E(1) to allow the AUSTRAC CEO to be able to place conditions on the registration of remittance providers. The measure is justified given that remittance providers are a high risk sector for money laundering and financing terrorism. These powers will mean the AUSTRAC CEO can take action to reduce these risks through imposing appropriate measures on remittance providers.

Dr Mark Zirnsak
Director
Justice and International Mission Unit
Synod of Victoria and Tasmania
Uniting Church in Australia

[17] John Gilkes, 'Open-Ended Intergovernmental Working Group on Asset Recovery. Asset Tracing and Recovery. A case study', 17 December 2010, http://www.unodc.org/documents/treaties/UNCAC/WorkingGroups/workinggroup2/2010-December-16-17/Presentations/John_Gilkes_StAR.pdf

Appendix 1. Case Studies of the Misuse of Virtual Currencies

1.1. Payment for Child Sexual Exploitation Material Online

The commercial trade in images of child sexual abuse involves hundreds of commercial child sex abuse sites. An estimated 50,000 new child sexual abuse images are produced each year.[18] The industry is estimated to be worth about US$250 million globally.[19] Reportedly a single child sexual abuse site can attract up to one million hits monthly.[20] The purchase and trade in commercial sexual abuse material generates a market and ongoing demand for the human rights abuses that are involved in the production of the material.

Commercial websites tend to cater to a specific group of offenders. They often have higher levels of extreme sexual abuse and sexual torture of children than images on non-commercial sites. Images are grouped in specific or narrow age ranges including categories for infants and toddlers, although this was a minority.[21] Just under a third of the images (29.7%) depict children being sexually assaulted, with 3.3% of images on commercial sites being of extreme sexual assaults compared to 2.7% of images on all child sexual abuse websites.

Trend data from the UK Internet Watch Foundation has shown the proportion of images of victims of child sexual abuse under the age of 10 has been decreasing in the last two years from 74% in 2011 to 81% in 2012 and 2013 to 69% in 2015 and 53% in 2016.[22] In 2016 2% of the images detected by the Internet Watch Foundation involved the sexual abuse of children aged two or under.[23] At the same time the proportion of images of child sexual abuse showing sexual activity between adults and children including rape and sexual torture decreased from 64% of images in 2011 to 53% of images in 2012 and 51% of images in 2013.[24]

The UK Internet Watch Foundation reported that in 2016 10% (5,452) of the 57,335 webpages confirmed as containing child sexual abuse imagery were commercial in nature, down from 24% (3,160) of the 13,182 webpages hosting child sexual abuse material in 2013.[25] However, while the proportion of commercial child sexual abuse sites has decreased there is a 73% increase in the actual number of such sites. Since 2009, the Internet Watch Foundation has identified 2,771 unique commercial brands of child sexual abuse material.[26] They found 575 brands were active in 2013, with 347 of these not having been seen before.[27] In 2016 there were 573 new commercial child sexual abuse businesses detected by the Internet Watch Foundation.[28] The analysis by the Internet Watch Foundation of hosting, payment arrangements, advertising systems and registration details suggested that these commercial websites are operated by a small core group of criminal entities.[29] Of the top 10 most prolific brands active during 2013, eight were apparently associated with a single 'top level' distributor and accounted for 15% of the total commercial content seen in

[18] UNODC, *The Globalization of Crime: A Transnational Organized Crime Threat Assessment* on 17 June 2010, p. 211, https://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf
[19] ibid, p. 211
[20] R. Wortley, Child Pornography. In: Natarajan M, editor. *International crime and justice*. USA: Cambridge University Press, 2010, p.178-84, cited in J. Pritchard et.al, 'Internet subcultures and pathways to the use of child pornography', *Computer Law and Security Review* 27, 2011, p.589
[21] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, p. 41.
[22] Internet Watch Foundation, 'Internet Watch Foundation Annual and Charity Report 2012', p. 11; Internet Watch Foundation, 'Internet Watch Foundation Annual & Charity Report 2013', p. 6; Internet Watch Foundation, 'IWF Annual Report 2016', p. 9.
[23] Internet Watch Foundation, 'IWF Annual Report 2016', p. 9.
[24] Internet Watch Foundation, 'Internet Watch Foundation Annual and Charity Report 2012', p. 11; and Internet Watch Foundation, 'Internet Watch Foundation Annual & Charity Report 2013', p. 6.
[25] Internet Watch Foundation, 'IWF Annual Report 2016', p. 18; and Internet Watch Foundation, 'Internet Watch Foundation Annual & Charity Report 2013', pp. 6, 17.
[26] Internet Watch Foundation, 'IWF Annual Report 2016', p. 19.
[27] Internet Watch Foundation, 'Internet Watch Foundation Annual & Charity Report 2013', p. 17.
[28] Internet Watch Foundation, 'IWF Annual Report 2016', p. 19.
[29] Internet Watch Foundation, 'Internet Watch Foundation Annual & Charity Report 2013', p. 17.

2013.[30] In 2016 the most prolific business accounted for 27% of commercial child sexual abuse material detected.[31]

It is reported that the UK Internet Watch Foundation has reported over 200 commercial child sexual abuse websites that accept Bitcoin for payment, with researchers in the US, Germany and other countries seeing the same.[32] The Internet Watch Foundation was quoted as saying that more than 30 sites accept only Bitcoin in 2014.[33] In 2016 the Internet Watch Foundation reported that 42 commercial child sexual abuse businesses were able to accept Bitcoin.[34]

Troels Oertling, the head of the cybercrime unit at Europol in The Hague is reported to have stated the UK based Ukash and Paysafecard, based in Vienna and backed by the EU, have been used to purchase online child sexual abuse material.[35]

The Financial Coalition Against Child Pornography was established in 2006 and involves 35 financial institutions and Internet industry bodies, along with the US National Centre for Missing and Exploited Children and its sister organisation, the International Centre for Missing and Exploited Children. Members include the Bank of America, Citigroup, Deutsche Bank, Google, HSBC – North America, Microsoft, Mastercard, Paypal, Visa, Western Union and Yahoo!. As a result of their efforts to block financial transactions involving commercial child sexual abuse site online, some of these sites are now refusing to process credit card payments from the US.

An Asia-Pacific Financial Coalition Against Child Pornography was established in 2009 and is based in Singapore. All providers of Australian merchant facilities for credit cards are involved in the Asia-Pacific Financial Coalition Against Child Pornography through the Australia card Risk Council being a member.

However, the new alternative payment systems that offer increased anonymity for both purchasers and purveyors of illegal content offer a new way to purchase online child sexual abuse material. As such, the emerging payment systems offer an appealing transaction option for illicit goods and services, including child sexual abuse images.[36]

The International Centre for Missing and Exploited Children believes there are clear indications that child sexual abuse material has moved to the "Virtual Shadow Economy" because it provides access to highly anonymous services for communications and payment.[37]

Commercial child sexual abuse sites are also supported by a range of payment methods to help avoid detection.[38] Payment systems may involve pre-pay cards, credit cards, 'virtual money' or e-payment systems and may be carried out across secure webpages, text or e-mail. A report by

[30] Internet Watch Foundation, 'Internet Watch Foundation Annual & Charity Report 2013', p. 17.
[31] Internet Watch Foundation, 'IWF Annual Report 2016', p. 19.
[32] Kristen Schweizer, 'Bitcoin Payments by Pedophiles Frustrate Child Porn Fight', http://www.businessweek.com/, 9 October 2014.
[33] Kristen Schweizer, 'Bitcoin Payments by Pedophiles Frustrate Child Porn Fight', http://www.businessweek.com/, 9 October 2014.
[34] Internet Watch Foundation, 'IWF Annual Report 2016', p. 19.
[35] Kristen Schweizer, 'Bitcoin Payments by Pedophiles Frustrate Child Porn Fight', http://www.businessweek.com/, 9 October 2014.
[36] Financial Coalition Against Child Pornography, 'Report on Trends in Online Crime and Their Potential Implications in the Fight Against Commercial Child Pornography', 1 February 2011, p. 2.
[37] International Centre for Missing and Exploited Children, 'A New Virtual Economy Poses New Challenges in Fighting Child Pornography and Child Exploitation', Media Release, 13 June 2013.
[38] Analysis by the Internet Watch Foundation (Annual and Charity report p.8) has identified that the criminals running these operations do so in a cluster of commercial child sexual abuse 'brands' from the manner in which they share hosting patterns, payment arrangements, advertising systems and registration details as well as from the overall appearance of the websites.

Cybetip.ca identified 27 different payment types.[39] The majority (85%) sold memberships, with recurring monthly payments ranging from $4 to $490 (an average of $53 a month). Membership could also be obtained for a one-time fee ranging from $30 to $1,990[40] with an average cost of $249.[41] DVDs were also sold for as much as $1,900. Other products include a variety of packages, image sets, videos and websites.[42] They concluded there is clearly a large consumer market for child sexual abuse images.

When Japan's Mt Gox, formerly the world's biggest Bitcoin exchange, shut down in April after a half-billion dollars of currency was stolen, US federal agents said the service had been used for about $60 million a month in payments for illegal products including child sexual abuse material.[43]

A UK commercial online child sexual abuse operation was estimated to have made £2.2 million through the distribution of millions of images. Their pages contained 121,654 images of child sexual abuse. Police were able to identify 1,511 suspected customers of the criminal operation.[44]

1.2. Liberty Reserve

The Liberty Reserve case demonstrates the vulnerability of unregulated virtual currencies for the purposes of money laundering. According to the case filled by the US Attorney for the Southern District of New York, Liberty Reserve SA operated one of the world's most widely used virtual currencies. Through its website, the Costa Rican company provided its customers with what it described as "instant, real-time currency for international commerce", which could be used to "send and receive payments from anyone, anywhere on the globe". The US authorities alleged that people behind Liberty Reserve:[45]

> *…intentionally created, structured, and operated Liberty Reserve as a criminal business venture, one designed to help criminals conduct illegal transactions and launder the proceeds of their crimes. Liberty Reserve was designed to attract and maintain a customer base of criminals by, among other things, enabling users to conduct anonymous and untraceable financial transactions.*
>
> *Liberty Reserve emerged as one of the principal means by which cyber-criminals around the world distributed, stored and laundered the proceeds of their illegal activity. Indeed, Liberty Reserve became a financial hub of the cyber-crime world, facilitating a broad range of online criminal activity, including credit card fraud, identity theft, investment fraud, computer hacking, child pornography, and narcotics trafficking. Virtually all of Liberty Reserve's business derived from suspected criminal activity.*
>
> *The scope of Liberty Reserve's criminal operations was staggering. Estimated to have had more than one million users worldwide, with more than 200,000 users in the United States, Liberty Reserve processed more than 12 million financial transactions annually, with a combined value of more than $1.4 billion. Overall, from 2006 to May 2013, Liberty Reserve processed an estimated 55 million separate financial transactions and is believed to have laundered more than $6 billion in criminal proceeds.*

A user opened an account through the Liberty Reserve website, and Liberty Reserve did not validate identities. Users routinely established accounts under false names, including blatantly

[39] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip.ca', November 2009, pp. 10, 56.
[40] This type was used by 15.4% of the sites.
[41] Canadian Centre for Child Protection, *op.cit*. p. 65.
[42] DVDs accounted for 5.8% of the sites, packages 4.7%, image sets 3.1%, videos 1.1% and websites 0.2%.
[43] Kristen Schweizer, 'Bitcoin Payments by Pedophiles Frustrate Child Porn Fight', http://www.businessweek.com/, 9 October 2014.
[44] Child Exploitation and Online Protection Centre, "Operation Alpine: Four main suspects sentenced today", 13 June 2011; and "Three jailed over £2.2 million internet child porn business", The Daily Mirror, http://www.mirror.co.uk/news/uk-news/three-jailed-over-22million-internet-134758.
[45] US Attorney for the Southern District of New York, 13 Civ 3565, 28 May 2013, pp. 4-5.

criminal names ("Russia Hackers", "Hacker Account", "Joe Bogus") and blatantly false addresses ("123 Fake Main Street, Completely Made Up City, New York"). To add a further layer of anonymity, Liberty Reserve required users to make deposits and withdrawals through recommended third-party exchangers – generally unlicensed money transmitting businesses operating in Russia and in several countries without significant governmental money laundering oversight or regulation at the time, such as Malaysia, Nigeria and Vietnam. By avoiding direct deposits and withdrawals from users, Liberty Reserve evaded collecting information about them through banking transactions or other activity that would create a central paper trail.[46]

It was further alleged by US authorities that for an additional "privacy fee" of 75 cents per transaction, a user could hide their own Liberty Reserve account number when transferring funds, effectively making the transfer completely untraceable, even within Liberty Reserve's already opaque system.[47]

Liberty Reserve had its own virtual currency, Liberty Dollars, but at each end, transfers were denominated and stored in fiat currency (US dollars).[48]

The investigation into Liberty Reserve involved law enforcement agencies from 17 countries, demonstrating the complexity of investigating global online crime operations involving virtual currencies.[49]

Australian entities became unwittingly caught up in Liberty Reserve's operations. Three Westpac bank accounts were amongst the 45 bank accounts the US obtained seizure warrants or restraining orders on.[50] US authorities sought to seize the assets in three Westpac accounts held by Technocash Ltd holding up to $36.9 million.[51] Technocash Limited was an Australian registered company. The funds are alleged to be connected to shell companies owned by the defendants in the case.[52]

US authorities alleged defendant Arthur Budovsky used Technocash to receive funds from exchangers. Mr Budovsky, the alleged principal founder of Liberty Reserve,[53] allegedly used his bank to wire funds to Technocash bank accounts held by Westpac.[54] He is also alleged to be the registered agent for Webdata Inc which held an account with SunTrust. Technocash records allegedly showed deposits into the SunTrust account from Technocash accounts associated with Liberty Reserve between April 2010 and November 2012 of more than $300,000.[55]

Arthur Budovsky is allegedly listed as the president for Worldwide E-commerce Business Sociedad Anonima (WEBSA) and defendant Maxim Chukharev as the secretary. Maxim Chukharev is alleged to have helped design and maintain Liberty Reserve's technological infrastructure.[56] WEBSA allegedly served to provide information technology support services to Liberty Reserve and to serve as a vehicle for distributing Liberty Reserve profits to Liberty Reserve principals and

[46] FATF, 'Virtual Currencies. Key Definitions and Potential AML/CFT Risks', June 2014, p. 10.
[47] US Attorney for the Southern District of New York, 13 Civ 3565, 28 May 2013, p. 6.
[48] FATF, 'Virtual Currencies. Key Definitions and Potential AML/CFT Risks', June 2014, p. 10.
[49] International Centre for Missing & Exploited Children and Thomas Reuters, 'The Digital Economy: Potential, Perils and Promises. A Report of the Digital Economy Task Force', March 2014, p. 15.
[50] US Attorney for the Southern District of New York, 13 Civ 3565, 28 May 2013, p. 10; and USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 43.
[51] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 29, 43.
[52] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 21.
[53] US Department of Justice, 'One of the World's Largest Digital Currency Companies and Seven of Its Principals and Employees Charged in Manhattan Federal Court and Running Alleged $6 Billion Money Laundering Scheme', 28 May 2013.
[54] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 29.
[55] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 36.
[56] US Department of Justice, 'One of the World's Largest Digital Currency Companies and Seven of Its Principals and Employees Charged in Manhattan Federal Court and Running Alleged $6 Billion Money Laundering Scheme', 28 May 2013.

employees.[57] It is alleged bank records showed that from July 2010 to January 2013, the WEBSA account in Costa Rica received more than $590,000 from accounts at Technocash associated with Liberty Reserve.[58]

It is alleged Arthur Budovsky was the president of Grupo Lulu Limitada which was allegedly used to transfer and disguise Liberty Reserve Funds.[59] Records from Technocash allegedly indicate that from August 2011 to November 2011 a Costa Rican bank account held by Grupo Lulu received more than $83,000 from accounts at Technocash associated with Liberty Reserve.[60]

Further, defendant Azzeddine El Amine, manager of Liberty Reserve's financial accounts,[61] was the Technocash account holder for Swiftexchanger. It is alleged e-mails showed that exchangers wishing to purchase Liberty Reserve currency wired funds to Swiftexchanger. When Swiftexchanger received funds in its Technocash account, an e-mail alert was sent to El Amine, notifying him of the transfer. Based on these alerts, it is alleged between 12 June 2012 and 1 May 2013, exchangers doing business with Liberty Reserve send approximately $36,919,884 to accounts held by Technocash at Westpac.[62]

The defendants are alleged to have used Technocash services to transfer funds to nine Liberty Reserve controlled accounts in Cyprus.[63]

Technocash Limited is reported to have been forced out of business in Australia following the action by US authorities, when it was denied the ability to establish accounts in Australia by financial institutions.[64] Technocash stated that it "complied with Australia's comprehensive AML [Anti-Money Laundering] regime, verified customers and has an AFSL licence since 2003. Technocash denies any wrong doing."[65]

1.3. Silk Road

In September 2013, the US Department of Justice unsealed a criminal complaint charging the alleged owner and operator of Silk Road, a hidden website designed to enable its users to buy and sell illegal drugs, weapons, stolen identity information and other unlawful goods and services anonymously and beyond the reach of law enforcement, with narcotics trafficking, computer hacking, and money laundering. The Department of Justice also seized the website and approximately 173,991 bitcoins, worth more than US$33.6 million at the time of the seizure, from seized computer hardware. The individual was arrested in San Francisco in October and indicted in February 2014.[66]

Launched in January 2011, Silk Road operated as a global black-market that brokered anonymous criminal transactions and was used by several thousand drug dealers and other unlawful vendors to distribute unlawful goods and services to over a hundred thousand buyers. It allegedly generated total sales revenue of approximately US$1.2 billion (more than 9.5 million bitcoins) and approximately US$80 million (more than 600,000 bitcoins) in commissions for Silk Road. Hundreds

[57] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 37.
[58] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 36.
[58] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 38.
[59] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 36.
[59] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 40.
[60] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 36.
[60] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 41.
[61] US Department of Justice, 'One of the World's Largest Digital Currency Companies and Seven of Its Principals and Employees Charged in Manhattan Federal Court and Running Alleged $6 Billion Money Laundering Scheme', 28 May 2013.
[62] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 30.
[63] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 31.
[64] Technocash, 'Opportunity: Own the Technocash Payment Platform', Media Release, 5 July 2013.
[65] http://www.technocash.com/pages/press-release.cfm
[66] FATF, 'Virtual Currencies. Key Definitions and Potential AML/CFT Risks', June 2014, p. 10.

of millions of dollars were laundered from these illegal transactions (based on bitcoin value as of dates of seizure). Commissions ranged from 8 to 15% of total sales price.[67]

Silk Road achieved anonymity by operating on the hidden Tor network and accepting only bitcoins for payment. Using bitcoins as the exclusive currency on Silk Road allowed purchasers and sellers to further conceal their identity, since sellers and recipients of peer-to-peer bitcoin transactions were identified only by the anonymous bitcoin address/account. Moreover, users were able to obtain an unlimited number of bitcoin addresses and use a different one for each transaction, further obscuring the trail of illicit proceeds. Users were also able to employ additional "anonymisers", beyond the tumbler service built into Silk Road transactions.[68]

1.4. Western Express International

An eight-year investigation of a multinational, Internet-based cybercrime group, Western Express Cybercrime Group, resulted in convictions or guilty pleas of 16 of its members for their role in a global identity theft/cyberfraud scheme. Members of the cybercrime group interacted and communicated primarily through Internet "carding" web sites devoted to trafficking in stolen credit card and personal identifying information and used false identities, anonymous instant messenger accounts, anonymous e-mail accounts, and anonymous virtual currency accounts to conceal the existence and purpose of the criminal enterprise; avoid detection by law enforcement and regulatory agencies; and maintain their anonymity.[69]

The criminal enterprise was composed of vendors, buyers, cybercrime service providers and money movers located in numerous countries, ranging from Ukraine and throughout Eastern Europe to the US. The vendors sold nearly 100,000 stolen credit card numbers and other personal identification information through the Internet, taking payment mostly in e-Gold and WebMoney. The buyers used the stolen identities to forge credit cards and purchase expensive merchandise, which they fenced (including via reshipping schemes), committing additional crimes, such as larceny, criminal possession of stolen property, and fraud, and generating about US$5 million in credit card fraud proceeds.[70]

The hub of the entire operation was Western Express International Inc, a New York corporation based in Manhattan that operated as a virtual currency exchanger and unregistered money transmitter to coordinate and facilitate the Internet payment methods used by the criminal enterprise, and to launder the group's proceeds. One of the largest virtual currency exchangers in the US, Western Express International exchanged a total of US$15 million in WebMoney and US$20 million in e-Gold for the cybercrime group and used banks and traditional money transmitters to move large sums of money. It also provided information and assistance through its websites (including Dengiforum.com and Paycard2000.com) on ways to move money anonymously and to insulate oneself from reporting requirements.[71]

Western Express International and its owner/operator, a Ukrainian national, pleaded guilty in February 2013 in New York State to money laundering, fraud and conspiracy offences. Three other defendants were convicted after trial in June 2013. Several more had pleaded guilty in August 2009.[72]

[67] FATF, 'Virtual Currencies. Key Definitions and Potential AML/CFT Risks', June 2014, p. 11.
[68] FATF, 'Virtual Currencies. Key Definitions and Potential AML/CFT Risks', June 2014, p. 11.
[69] FATF, 'Virtual Currencies. Key Definitions and Potential AML/CFT Risks', June 2014, p. 12.
[70] FATF, 'Virtual Currencies. Key Definitions and Potential AML/CFT Risks', June 2014, p. 12.
[71] FATF, 'Virtual Currencies. Key Definitions and Potential AML/CFT Risks', June 2014, p. 12.
[72] FATF, 'Virtual Currencies. Key Definitions and Potential AML/CFT Risks', June 2014, p. 12.