e-finance&payments law&policy

THE NEWSLETTER FOR THE E-FINANCE INDUSTRY
JUNE 2013 VOLUME 07 ISSUE 06
WWW.E-COMLAW.COM

Liberty Reserve indictment rocks digital currency world

The indictment sealed on 20 May by a Grand Jury in the Southern District of New York, charging defendants operating international online digital currency and money transfer service Liberty Reserve with conspiracy to commit money laundering and operate an unlicensed money transmitting business, has raised questions about the future of digital currencies like Bitcoin.

The shutting down of Liberty Reserve "has sent a shudder through the digital currency world," said Kevin L. Petrasic, Partner at Paul Hastings. "What that means for the continued growth and proliferation of digital currencies remains to be seen. Clearly, an issue that digital currencies must consider is the use of such currencies as a platform to promote anonymity that encourages money laundering activities."

Described by the DoJ as the 'largest international money laundering prosecution in history,' according to the indictment papers it is estimated that 55 million transactions were processed and more than $6 billion of 'criminal proceeds' laundered. Established in Costa Rica in 2006, Liberty Reserve enabled users to conduct anonymous international transactions with its own digital currency.

"Many of the issues presented by the Liberty Reserve digital currency are present with Bitcoin, and we have certainly heard speculation about what the indictment and accompanying FinCEN rule to 'seal off' Liberty Reserve from US financial institutions could mean for Bitcoin," adds Petrasic. "The challenge for Bitcoin and digital currencies will be to try to figure out how to detect and track money laundering activities. Succeeding in doing so will restore credibility in the AML context and avoid doubts about the ability of such currencies to survive and remain viable."

"It's surprising that FinCEN took such a strong position on payment finality," said Ryan J. Straus, Attorney at Graham & Dunn. "In noting that Liberty Reserve was a completely irrevocable payment system and digital currency, FinCEN stated that irrevocability makes for a 'highly desirable system for criminal use and a highly problematic one for legitimate payment functions.'" Concludes Craig Denney, Of Counsel at Snell & Wilmer LLP, "Any entities involved in the digital currency transaction business should be concerned. This indictment should make companies take notice and examine what due diligence protocols they have implemented to know their customers."

Australian watchdog proposes single NFC regulatory framework

Australia's Communications and Media Authority's (ACMA) 6 June paper, 'Near-field communications: emerging issues in media and communications,' has called for a single regulatory framework for NFC.

"NFC solutions touch on a number of different regulatory frameworks," explains Cheng Lim, Partner at King & Wood Mallesons. "A single framework would require significant co-ordination across a number of government regulators and potential legislative changes. It would offer potential benefits, particularly if it relaxed the financial services and banking-related regulatory requirements for services that provide for only low-value transactions."

The ACMA argues that current regulations do not entirely address NFC, resulting in uncertainty. A single framework, it says, alongside 'co- and self-regulatory arrangements,' would increase consumer protection and NFC growth.

Lim highlights the lack of incorporation of NFC by Apple as an example of a challenge affecting NFC growth, but adds that "most [challenges] appear to be commercial rather than regulatory challenges."

"I do not see that, presently, there is a case for more extensive NFC-specific regulation," believes Stephen Cavanagh, Partner at HWL Ebsworth Lawyers. "There are arguably more relevant [payments regulation] issues warranting consideration, such as whether Part 7.8 of the Corporations Act should be amended to clarify whether it is intended to apply to stored value products and, if so, how."

Fragmentation security risk to smartphones

A report, commissioned by Ofcom and produced by Goode Intelligence, has highlighted how supply chain fragmentation and the presence of numerous players in smartphone value chains is a key problem affecting smartphone security.

"Multiple players and fragmentation is one of the primary causes of the lack of and/or of delayed software updates to consumers' smartphones," explains Alan Goode, Managing Director at Goode Intelligence. "This results in handsets left vulnerable to criminal exploitation."

The research, 'Study into the implications of Smartphone operating system security,' examines ten areas of security including app store security and UK consumer protection practices in this area.

"Evidence suggests current levels of consumer harm in the UK are low," said Goode. "However, market practices create a potential vulnerability. If not addressed, the problem will increase. What is applicable for smartphone OS security and software updates is true for other internet connected systems and embedded OS, such as wearable devices."

IN THIS ISSUE