CYPRUS ADVERTISING REGULATION ORGANIZATION

DECISION

FIRST INSTANCE JURY

ID	**A-017**
Complaint by	**Consumer**
Advertiser	Neo & Bee
Issue	Claim on TV spot
Discussed on	Tuesday 11 March 2014
RESERVE Judgement Issued	**Thursday 13 March 2014**
FINAL Decision issued	**Wednesday 19 March 2014**

Jury Assessment:

1. The jury noted the independent data provided by Neo. It notes that both opinions provided *confirm* the existence of the two instances referred to in its reserve judgement of 13.3.2014. It also notes that the advertiser's argument for "absolute security of transactions" rested entirely on the technology behind the bitcoin protocol and the view that a breach in that protocol is extremely improbable. However, despite the minimal consequences of the two instances referred to and the fact that they were resolved quickly, it is also a fact that during the relatively brief bitcoin history, there have been at least two instances in which the integrity of the core bitcoin protocol was brought into question.

2. From all the information presented before the jury, the conclusion that flows is that *by design* the bitcoin software facilitates transactions that, once created, cannot be changed or fail, and in order for that to happen, something "arbitrary" and/or "extremely improbable" must occur. As we understand, this quality is the basis of the advertiser's claim of "absolute security of transactions". However, given the two instances referred to, it is obvious that at least two unanticipated events did occur.

3. Given the above, the jury considers that the claim of *"absolute security"* in bitcoin transactions has not been proven and is thus in breach of **article 8** of the Code of the Cyprus Advertising Regulation Organization which states that *"Descriptions, claims or illustrations relating to verifiable facts in a marketing communication should be capable of substantiation"*. It should therefore be **amended -in all media and ads- within the timeframes specified in the Committee's rules (Article 7).**

Finally, the Committee would like to exercise its right (Article 5, paragraph λ of its rules of operation) to **review any new claim on safety *before the latter is aired/published so as to confirm compliance***. The decision on compliance will be taken within two working days of the receipt of the proposed changes.

CYPRUS ADVERTISING REGULATION ORGANIZATION

RESERVE DECISION

FIRST INSTANCE JURY

Complaint by	**Consumer**
Advertiser	Neo & Bee
Issue	Claim on TV spot
Discussed on	Tuesday 11 March 2014
Reserve Decision issued	**Thursday 13 March 2014**

Issue:

XX complained that the ad claims that the consumer handles his/her finances *with absolute safety*. However, it is known that there is no absolute safety in the bitcoin currency. How can the claim of absolute safety be accepted when Mt. Gox, a bitcoin "bank" in Japan, was broken into and filed for bankruptcy? Moreover, if safety refers to the relative stability in the value of bitcoins, the volatility in the exchange prices to date cannot lead support to this claim.

The ad copy follows:

> Ποιος είναι ο Neo?
> #whoisneo
>
> - Εγώ είμαι ο Neo!
> - Εγώ είμαι ο Neo!
> - Κι εγώ είμαι ο Neo!
> - Κι εγώ είμαι ο Neo!
> - Κι εγώ είμαι ο Neo!
> - Εγώ είμαι ο Neo!
> - Εγώ είμαι ο Neo!
>
> Neo. Ήρθε κι αλλάζει τη ζωή μας.
> Η εταιρεία που με την τεχνογνωσία της φέρνει το ψηφιακό νόμισμα Bitcoin στη ζωή μας
> κι έτσι ο έλεγχος των χρημάτων μας έρχεται στα δικά μας χέρια.
> Συναλλαγές σε όλο τον κόσμο
> ΧΩΡΙΣ ΚΑΝΕΝΑ ΠΕΡΙΟΡΙΣΜΟ ΚΑΙ ΜΕ ΑΠΟΛΥΤΗ ΑΣΦΑΛΕΙΑ
> Τώρα με τη Neo και το δίκτυο πληρωμών Bee
> ΚΑΝΟΥΜΕ ΟΛΕΣ ΤΙΣ ΣΥΝΑΛΛΑΓΕΣ ΚΑΙ ΑΓΟΡΕΣ ΜΑΣ
> ΧΩΡΙΣ ΕΠΙΠΛΕΟΝ ΧΡΕΩΣΕΙΣ!

Neo! Bee the change

Μάθετε περισσότερα 77776544
www.neo-bee.com

Advertiser's Response:

- The claim of "**absolute safety**" in the ad is explicitly tied -and limited to- **transactions** in bitcoins. In layman's terms, bitcoin transactions/"movements from A to B" are completely safe and cannot be tampered with; they are final once executed. As with all other currencies, including fiat currencies, the possibility of theft from the place of storage cannot be ruled out. However, that is not the claim in the ad. The fact that somebody can steal one's bitcoin security keys and gain access to their "wallet" is a different thing to the safety of the transactions.
- The bitcoin protocol by its design ensures that transactions are completely secure. The downfall of Mt. Gox –or of other exchanges/bitcoin storage institutions- does not reflect on the transactional safety of bitcoins and should not be confused with the technology behind the protocol. Arguing that bitcoin transactions are unsafe because Mt. Gox –a bank pool of bitcoins- failed, is akin to arguing that transactions in euros are unsafe because of the failure of a bank (such as Laiki bank).
- Bitcoin is a digital currency founded on certain core principles: it is created on a peer-to-peer network, using open source software with total supply predefined and capped at 21 million. The peer-to-peer network guarantees that the network is always running, so as long as the internet exists and we don't have a total internet blackout, transactions will take place. Open source codes are perfectly transparent and as safe as it goes -in computing there is nothing impossible; however, it is valid to claim that a breach in the transactional safety of bitcoin is extremely improbable.
- Bitcoin has a sound basis in cryptography. SHA256 and ECDSA which are used in Bitcoin are well-known industry standard algorithms. If these algorithms are deemed untrustworthy then one should not trust Bitcoin, credit card transactions or any type of electronic bank transfer.
- Although this is not the claim in the ad, Neo has taken measures to enhance bitcoin "wallet" security: Neo offers its customers a set of 3 "keys", 2 of which are needed to access an account. One key is held by the client, the other by Neo and the third by another company (not named to the Committee but known to customers when they sign up). All three parties are bound by contractual agreement; therefore even if something happens to Neo, the customer will still be able to access their bitcoins through the use of his/her private key and the key of the third party. In addition to that, Neo has seven corporate policies in place to address issues such as risk management, money laundering etc., and is lobbying hard for regulation of bitcoin based businesses. Moreover, Neo invests significant time and energy to educate their clients on the specifics of bitcoin economy, in order to minimise risks that are inherent in all monetary affairs and allowing them to assume responsibility for their finances.
- Regarding the argument that bitcoin exchange prices with fiat currencies have to date proved very volatile - again *this is not the claim in the ad*. Furthermore, there is no absolute value in anything monetary and Neo has never stated that bitcoin currency exhibits a quality which no other currency in the world has.

Jury Assessment:

1. The jury noted the argumentation put forward by Neo. It understands that the claim, as presented in the ad, refers to and is limited to **security of transactions** in the bitcoin currency and that this claim differs from wallet security. The question therefore is whether there can be *"absolute security"* in bitcoin transactions. In the jury's mind, absolute claims hold a very high standard of proof. The essence of the question before the committee was whether the word absolute in this claim denotes the *impossibility* of bitcoin transactional safety and protocol being compromised, or the *extreme improbability* of that happening.

2. The discussion before the Committee -and the thrust of the argumentation by Neo- was that bitcoin protocol security should not be confused with the security standards of various exchanges (such as Mt. Gox, etc). It is the latter that were violated with the result of loss/theft of bitcoins; however, bitcoin protocol is what underpins security of transactions in bitcoins.

3. As we understand from Wikipedia and other references, **at least two incidents** of transactional safety being compromised due to the bitcoin protocol have taken place to date in the relatively brief bitcoin history. Quoting from Wikipedia:

> *On 6 August 2010, a major vulnerability in the Bitcoin protocol was spotted. Transactions weren't properly verified before they were included in the transaction log or "block chain" which let users bypass Bitcoin's economic restrictions and create an indefinite number of bitcoins. On 15 August, the vulnerability was exploited; over 184 billion bitcoins were generated in a transaction, and sent to two addresses on the network. Within hours, the transaction was spotted and erased from the transaction log after the bug was fixed and the network forked to an updated version of the Bitcoin protocol. This was the only major security flaw found and exploited in Bitcoin's history.*
>
> *On 12 March 2013, a Bitcoin miner running version 0.8.0 of the Bitcoin software created a large block that was incompatible with earlier versions of the Bitcoin software because of its size. This created a split or "fork" in the block chain since older versions of the software did not accept this block as valid. Computers with the recent version of the software accepted the block and continued to build on the diverging chain, whereas older versions of the software rejected it and continued extending the block chain without the offending block. This split resulted in two separate transaction logs being formed without clear consensus, which allowed for the same funds to be spent differently on each chain.*
> *In response, the Mt. Gox exchange temporarily halted Bitcoin deposits. The exchange rate fell 23% to $37 on the Mt. Gox exchange but rose most of the way back to its prior level of $48. Developers at bitcoin.org resolved the split by recommending that users downgrade to "version 0.7", which utilized the oldest transaction log in the split. User funds largely remained unaffected and were available when network consensus was reached. The network reached consensus and continued to operate as normal a few hours after the split.*

4. The LMB Holdings prospectus used to raise capital to fund Neo and the Bee Payment Network (available today on the website of LMB Holdings, https://www.lmb-holdings.com/public_ledger/) also references the 2013 incident (*page 19*, under title Bitcoin vulnerabilities):

> *Bitcoin Vulnerabilities*
> *The primary cryptographic algorithm used in Bitcoin is SHA256. SHA256 is used and trusted in many online security protocols, including TLS, SSL, and PGP. Though a compromise in SHA256 would jeopardize the security of most popular online services, such as Facebook, Gmail, and PayPal, the Bitcoin protocol can shift to a stronger algorithm. Though the mass update across the entire network required to change algorithms would destabilise the network and the Bitcoin economy for a period, the effect would be akin to an exchange halting trading: Bitcoins would be "frozen" for up to a couple of days while the update is released. Though this would be frustrating, if SHA256 is compromised, the rest of the online world would be devastated as users are no longer able to securely log in to their services.*
> *Neo will employ systems to detect a fork occurring on the Bitcoin network to mitigate double-spend attacks. As many transfers will be processed internally, not on the blockchain, only external Bitcoin deposits and withdrawals would have to be suspended: all fiat bank functions, as well as internal Bitcoin transactions, will be able to continue uninterrupted. As soon as the network issue is resolved, Neo can send any pending transactions from the downtime to the Bitcoin network.*
> *A hard fork occurred on May 15th 2013 and was resolved within a matter of hours. The previous occurrence of a hard fork demonstrated the openness and the ability of the Bitcoin community as a whole to address issues in a timely manner.*

5. The Committee notes that when Neo was asked if, during the years of bitcoin existence there has ever been an instance of transaction failure, their reply was that throughout its 5 years of existence there has never been a case of a transaction that failed and that fact is verifiable. Asked if that verification can be sourced from independent third parties, the answer was positive.

6. Taking into account the highly technical nature of the discussion and with the aim to do justice to the advertiser, **the Committee reserves judgement** (Article 6, paragraph γ of its rules of operation) and will reassess the issue upon receipt **within 48 hours** of

a) data from **independent, third party sources** which give a different perspective. Any expense incurred in procuring this data should be borne by the advertiser.

b) an explanation for the two instances mentioned above.

During these 48 hours, the ad may continue to air as is (Article 6, paragraph δ of its rules of operation).