

COMPLAINT NUMBER	19/026
COMPLAINANT	F Zinsli and B Sharp
ADVERTISER	NordVPN
ADVERTISEMENT	NordVPN, Television
DATE OF MEETING	26 February 2019
OUTCOME	Not Upheld

SUMMARY

The NordVPN television advertisement says “Every time you’re on-line your private information can be stolen, sold or exploited. That’s why you need NordVPN. On-line protection trusted by millions of people worldwide. NordVPN uses military grade encryption that protects your information from on-line tracking. In just a few clicks protect up to 6 devices for the limited time offer of just \$2.99 US per month...”

Two complaints were received about this advertisement. F Zinsli said the advertisement is misleading to quote pricing in US Dollars and is misleading in its representation of the security it offers because once the user’s connection leaves the VPN, there is no protection.

B Sharp said the reasons given in the advertisement for purchasing the product are overstated. They say the product doesn’t protect against information theft and there is no real risk to users as most websites use the HTTPS secure protocols.

The Advertiser responded to each point made by the Complainants. It explained the protection offered by a VPN product and substantiated the claims made in the advertisement.

The Complaints Board said the advertisement was not likely to mislead or deceive consumers in terms of pricing, the level of security on offer or the value of its services.

The Complaints Board said the advertisement had been prepared with a due sense of social responsibility and ruled the advertisement was not in breach of Basic Principle 4 or Rule 2 of the Code of Ethics.

The Complaints Board ruled the complaint was Not Upheld

[No further action required]

Please note this headnote does not form part of the Decision.

COMPLAINTS BOARD DECISION

The Chair directed the Complaints Board to consider the advertisement with reference to Basic Principle 4 and Rule 2 of the Code of Ethics.

Basic Principle 4 required the Complaints Board to consider whether the advertisement had been prepared with a due sense of social responsibility to consumers and to society.

Rule 2 required the Complaints Board to consider whether the advertisement contained any statement or visual presentation or create an overall impression which directly or by implication, omission, ambiguity or exaggerated claim is misleading or deceptive, is likely to deceive or mislead the consumer, makes false and misleading representation, abuses the trust of the consumer or exploits his/her lack of experience or knowledge.

The Complaints Board ruled the complaint was Not Upheld.

The Complaints

Two complaints were received about this advertisement. F Zinsli said the advertisement is misleading to quote pricing in US Dollars and is misleading in its representation of the security it offers because once the user's connection leaves the VPN, there is no protection.

B Sharp said the reasons given in the advertisement for purchasing the product are overstated. They say the product doesn't protect against information theft and there is no real risk to users as most websites use the HTTPS secure protocols.

The Advertiser's Response

The Advertiser responded to each point made by the Complainants. It explained the protection offered by a VPN product and substantiated the claims made in the advertisement.

The Media's Response

The Commercial Approvals Bureau said the currency used was clearly displayed and overseas currency fluctuations made it necessary to use US Dollars for clarity.

The Complaints Board Discussion

Consumer takeout

The majority of the Complaints Board said the likely consumer takeout of the advertisement is that installing a VPN system will help to protect key information if you are concerned about online security. The cost is US dollars \$2.99 per month.

A minority of the Complaints Board said some consumers could interpret the online security offer to protect your private information to mean the product will protect against credit card and password theft.

Is the use of foreign currency in the advertisement misleading?

The Complaints Board referred to a precedent Decision 18/411, which dealt with the issue of foreign currency for the same advertisement and was ruled No Grounds to Proceed by the Chair of the Complaints Board. That Decision said in part:

“The Chair said the advertisement had stated both verbally and on screen the cost was in US Dollars. In the Chair's view, this made the price and currency clear and the advertisement was not likely to mislead consumers.”

The Complaints Board agreed with this decision and said that it was common for online shopping sites to use international currencies to offset the risks relating to currency fluctuation. The Board said as the basis for the pricing was clear in the advertisement, consumers were unlikely to be deceived or misled.

Is the security offer made in the advertisement misleading?

The Complaints Board said the Nord VPN Virtual Private Network product routes the user's internet traffic through a remote server as a way of hiding IP address and encrypting all incoming and outgoing data.

The Complaints Board said a key message in the advertisement was the statement that "Nord VPN uses military grade encryption that protects your information **from online tracking.**" The Board said there was no claim made in the advertisement the product could protect against the threat of credit card or password theft. The Complaints Board agreed the product advertised was one of the tools consumers could use to support their online security and was likely to be used in conjunction with others – for example - a virus protection product.

A minority of the Complaints Board said it may have been useful for the Advertiser to differentiate the identity information its product protects, from the wider online security issue of personal information theft. However, on balance the Complaints Board were unanimous that the advertisement was not misleading about the level of security its product offered.

Is the advertisement overstating the need for this level of security?

The Complaints Board noted the substantiation provided by the Advertiser as to why using its product gives greater protection than relying on HTTPS secure protocols. The Board accepted the Advertiser's information that these were benefits. The Complaints Board agreed there was growing concern from consumers about devices being tracked and there could be a market for protecting IP addresses. Therefore, the Complaints Board did not consider the advertisement was overstating the security concerns of the general public.

In summary, the Complaints Board unanimously agreed the advertisement was not likely to mislead or deceive consumers in terms of pricing, the level of security on offer or the services it provides. The Board said the advertisement had been prepared with a due sense of social responsibility and ruled the advertisement was not in breach of Basic Principle 4 or Rule 2 of the Code of Ethics.

The Complaints Board ruled the complaint was Not Upheld.

DESCRIPTION OF ADVERTISEMENT

The NordVPN television advertisement says "Every time you're on-line your private information can be stolen, sold or exploited. That's why your need NordVPN. On-line protection trusted by millions of people worldwide. NordVPN uses military grade encryption that protects your information from on-line tracking. In just a few clicks protect up to 6 devices for the limited time offer of just \$2.99 US per month..."

COMPLAINT FROM F ZINSLI

This advertisement shows the product in US dollars. We are not in the USA, nor does NZ trade in US dollars for its products or services, any advertisement should be priced in the currency of the country being advertised in.

The product advertised makes claims of military grade encryption the is capable of protecting the clients data. This I do not dispute. However, what I do dispute is the nature of the product they are advertising. It is a VPN (Virtual Private Network) which works as a point to point private tunnel between the client and the server. But once the connection leaves the confines of the NordVPN network the VPN tunnel offers zero protection and the customers data cannot be protected.

Therefore: whilst the client is connected to the NordVPN network all data is protected. However, once a client makes a request for data that is outside the NordVPN network (most commonly a website) that connection cannot be protected unless NordVPN have a dedicated VPN tunnel to the web server in question. NordVPN would need to have a dedicated VPN connection to every server in the world to be able to achieve this.

Therefore the advertisement is misleading in its representation of security.

COMPLAINT FROM B SHARP

NordVPN advertises their product using misinformation and I believe this is harmful to the general public. They claim by ambiguity that general browsing can lead to attacks, exploits, and theft of their data, which implies debit cards and credentials. VPNs do no such thing, A VPN does not protect against information theft, and by using one not operated by yourself, you risk them accessing your information if that data is unencrypted. All websites are being encouraged to use HTTPS secure protocols nowadays anyway, so the premise on which this advert operates is null and void, as the only source of an attack is from within the website's infrastructure or on the user's machine, which cannot be protected against using a VPN.

Information such as browsing location, which is vague and approximate, can be determined by intermediate parties such as your ISP, but this isn't a privacy concern to many. This data is used to route traffic on every website you visit, and one should really only be concerned about this if partaking in illegal activities.

The points made in this advert as reasons to purchase the product are misleading and damaging to the public, many of which are uninformed in this area.

CODES OF PRACTICE

CODE OF ETHICS

Basic Principle 4: All advertisements should be prepared with a due sense of social responsibility to consumers and to society.

Rule 2: Truthful Presentation: - Advertisements should not contain any statement or visual presentation or create an overall impression which directly or by implication, omission, ambiguity or exaggerated claim is misleading or deceptive, is likely to deceive or mislead the consumer, makes false and misleading representation, abuses the trust of the consumer or exploits his/her lack of experience or knowledge. (Obvious hyperbole, identifiable as such, is not considered to be misleading).

RESPONSE FROM ADVERTISER, NORDVPN

1. Complaint by F Zinsli, Sunday, December 23, 2018 3:13 PM

1.1. "This advertisement shows the product in US dollars. We are not in the USA, nor does NZ trade in US dollars for its products or services, any advertisement should be priced in the currency of the country being advertised in."

RESPONSE: Complaint regarding the US dollars currency used in NordVPN TV advertisement was already addressed in Chair's Ruling: Complaints No Grounds to Proceed, complaint No. 18/411.

1.2. "Whilst the client is connected to the NordVPN network all data is protected. NordVPN would need to have a dedicated VPN connection to every server in the world to be able to achieve this. Therefore the advertisement is misleading in its

representation of security. However, once a client makes a request for data that is outside the NordVPN network (most commonly a website) that connection cannot be protected unless NordVPN have a dedicated VPN tunnel to the web server in question".

RESPONSE: A VPN encrypts all user's Internet traffic upon leaving a device. Traffic then is routed through an encrypted tunnel, sort of an alternative path from the one, provided by the ISP and sent to a VPN server, along with thousands of other people, making countless different requests at the same time.

After reaching the VPN server, each connected individual is provided with the same IP address, different from the one assigned by ISP. This makes virtually impossible to link any Internet activity to the particular user when traffic leaves our VPN servers. Hacker gets no use from knowing the public IP of a user as it can only be traced back to the VPN server.

Data outside of the NordVPN server is further protected by the TLS protocol if the destination website uses HTTPS. However, in cases the destination website is not using HTTPS, NordVPN has a "CyberSec" feature, which when enabled, will prevent user devices from communicating with botnet C&C center and from accessing malicious/phishing websites.

This way VPN grants a private and safe way of using the Internet on both, private and public networks: <https://gizmodo.com/5990192/vpns-what-they-do-how-they-work-and-why-youre-dumb-for-not-using-one>

2. Complaint by B Sharp, Monday, December 31, 2018 5:50 PM

2.1. "A VPN does not protect against information theft, and by using one not operated by yourself, you risk them accessing your information if that data is unencrypted."

RESPONSE: A VPN will not protect against information theft if the malware is already pre-installed on a device or a user enters his details on a phishing site. However, VPN solution makes it virtually impossible for malicious actors to access/intercept user data while traffic is traveling from the device to the destination on the internet. Also, the encryption ciphers we use in our apps are approved by multiple government agencies around the world (including NSA) to be used for encrypting top secret information. By now, there is no known proof of concept to break these ciphers, at least not with the current technology.

2.2. "All websites are being encouraged to use HTTPS secure protocols nowadays anyway, so the premise on which this advert operates is null and void, as the only source of an attack is from within the website's infrastructure or on the user's machine, which cannot be protected against using a VPN."

RESPONSE: HTTPS will encrypt information you enter into a website; however, it will not disguise your location or offer any privacy protection. It will also not offer any defence against internet censorship like a VPN does.

Moreover, sources of an cyber attack are not only websites or user devices. Data interception may also occur when someone stands in between the traffic source and the destination website. It is often the case with phishing sites. However, when the source or 'client' is connected to NordVPN, such interception becomes impossible. That is because user data travelling from the device to our VPN servers is encrypted, and after data leaves our VPN server, each connected individual is provided with the same IP address of a VPN server. Also, our CyberSec feature prevents from data theft by blocking an access to known phishing sites in the first place.

2.3. "Information such as browsing location, which is vague and approximate, can be determined by intermediate parties such as your ISP, but this isn't a privacy concern to many. This data is used to route traffic on every website you visit, and one should really only be concerned about this if partaking in illegal activities."

RESPONSE: Having your IP address visible to the public may not seem like a privacy concern at first. However, almost all websites that you visit track visitor IP addresses. As a result, they then use these IP addresses together with other attributes at hand to create very accurate user profiles, which as a result can lead to the loss of privacy.

RESPONSE FROM MEDIA, COMMERCIAL APPROVALS BUREAU

NORD VPN TELEVISION ADVERTISEMENT

COMPLAINT: 19/026

KEY: NVPN0300002

RATING:

G

We have been asked to respond to this complaint under the following codes:
Code of Ethics – Basic Principle 4, Rule 2

CAB approved this Nord VPN commercial on 28/10/18 with an 'G' general classification.

There appears to be two main issues arising from the received complaints:

1. The quoted price in U.S. dollars
2. The technical details of this complex product

The commercial quotes a monthly subscription cost is U.S. dollars, which is clearly marked in both the on-screen graphics and aurally in the voice-over.

International currencies are a fact of life on the global, interconnected marketplace of the internet. Quoting an NZD price would be disingenuous due to the constant fluctuation of exchange rates. The advertiser has very clearly demarcated the currency in which a customer will be charged, and in doing so has met a due standard of social responsibility.

With regards to the technical functions and possible limitations of the advertised product, CAB will defer to the expertise of the advertiser themselves.

APPEAL INFORMATION

According to the procedures of the Advertising Standards Complaints Board, all decisions are able to be appealed by any party to the complaint. Information on our Appeal process is on our website www.asa.co.nz. Appeals must be made in writing via email or letter within 14 days of receipt of this decision.