Common position of national authorities of the CPC Network concerning the commercial practices of Shopify

Under the Consumer Protection Cooperation (CPC) Regulation (EU) 2017/2394[1], Member State authorities[2], with the facilitation of the European Commission, have the duty to work together to enforce EU consumer law in the Single Market. CPC authorities, with the Belgian DG for Economic Inspection acting as a coordinator, have taken the following common position regarding the protection of consumers using Shopify web shops.

This common position is without prejudice to any other legal issues that national authorities may want to raise or may have raised in national proceedings.

1. Introduction

Shopify is a multinational e-commerce business that enables traders to create their own fully functional online stores[3] through a simple interface.

Shopify takes care of web hosting, domain name purchases and helps in quickly setting up an online store by providing a variety of services such as SSL certificates, payment gateways, store management, analytics, marketing and search engine optimization.

During the Covid-19 crisis, the popularity of the Shopify platform has increased due to traders looking for a fast solution to set up a web shop[4]. Unfortunately, also the problem of web shops engaging in unfair commercial practices has been intensified in the context of the Covid-19 crisis[5].

Within the member states of the CPC authorities, the scale of the problem has become an important issue. For example, the Belgian European Consumer Centre (ECC Belgium) received 686 requests in 2020 related to Shopify web shops and already 1140 requests up to 24 June 2021. As such, issues with Shopify web shops have become the number two complaint area of ECC Belgium.

2. Unfair commercial practices facilitated through Shopify

It emerges from its business model that the activities of Shopify have a direct relevance and a considerable impact on the "business-to-consumer commercial practices" carried out by third parties using Shopify products and services. Even though its products/services are primarily used by traders, the templates and features that Shopify provides to build an online store are at the same time

[1] Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No 2006/2004, OJ L 345, 27.12.2017, p. 1–26.
[2] The Consumer Protection Cooperation (CPC) network consists of authorities responsible for enforcing EU consumer protection laws in EU-27/EEA Member States, including Norway, Iceland and Liechtenstein.
[3] These can include web shops, but also other online sales channels such as apps and social media.
[4] Financial Times, "Shopify doubles sales for third consecutive quarter", https://www.ft.com/content/634d8560-49e6-4874-bbeb-125e900823ff.
[5] Financial Times, "Thousands of fraudsters are selling via Shopify, analysis finds", https://www.ft.com/content/0280592d-0adf-4dcb-a831-4f8a85f414bc.

published and directly addressed to consumers for the promotion and sales of products. Consequently, it is exclusively through Shopify's products (pre-designed websites and tools) that the consumer can actually have access to the products of the traders who create online stores through the Shopify platform. As such, Shopify has a major and direct influence on the Business-to-Consumer (B2C) practices of its traders and their ability to abide to EU consumer law.

As a facilitator, Shopify is in a unique position to make sure that traders can set up a web shop in compliance with EU consumer law ("compliance by design"). Only through ensuring that its website and legal templates, plug-ins and apps take into account basic EU consumer law requirements (such as company identification, the right of withdrawal and consumer guarantees), Shopify can enable traders that use the platform to act in compliance with EU consumer law.

This way, Shopify can support its traders as a diligent economic operator and, in many cases, it can prevent the necessity of any actions of CPC authorities against its customers that infringe on EU consumer law (e.g. notice and action requests towards Shopify as a hosting service, see par. 3).

The current design of certain tools offered by Shopify facilitates a long list of unfair commercial practices that are analysed here below. The company should adapt or ban those tools that are in high risk of misleading consumers and should warn the traders about the legal limitations as regards the use of Shopify's tools vis-à-vis EU consumers.

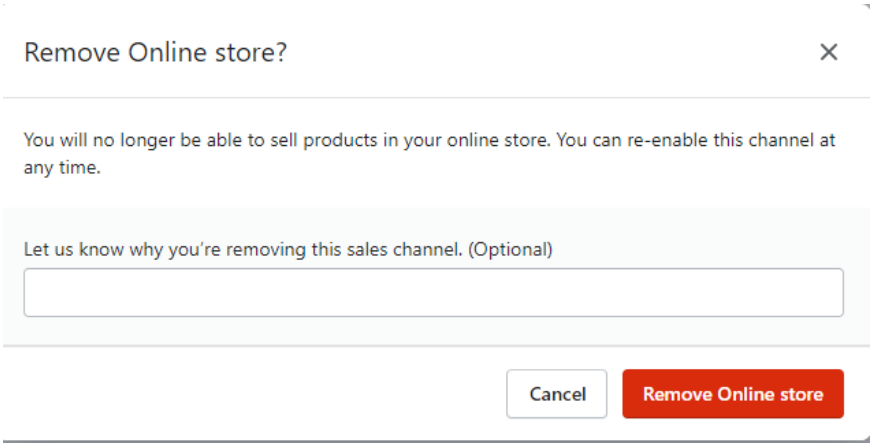
2.1. Lack of company identification

Both the European e-Commerce Directive, the Consumer Rights Directive and the Unfair Commercial Practices Directive contain the obligation for traders to **clearly mention their company identification and contact details** (company name, geographic address, electronic mail address, company number and VAT number). These company details are vital for consumers, both before and after the purchase, to be able to identify the trader upfront and to exercise their basic rights like the right of withdrawal and consumer guarantees. If a consumer does not know which trader sold the goods, he cannot exercise any of these basic rights.

CPC authorities noticed several Shopify web shops using Terms & Conditions templates with mentions like "*Company identification / company number: on demand*" and only an email address mentioned. This is a clear infringement of European consumer protection law as the information needs to be publicly provided upfront and not only on demand.

As Shopify offers different templates to traders to start their web shop, Shopify is in a unique position to make sure traders are reminded of their basic legal obligations. For example, the default contact page could be adapted to not only mention an e-mail address and/or contact form, but also the company identification details.

Finally, as Shopify traders need to pay per active web shop, CPC authorities notice that traders often remove their web shops after just a few months of activity to start a new one. Traders can easily remove their online store by clicking on the corresponding tab.



Consumers who bought goods on these online stores and try to revisit them, only get a Shopify error page. This way, consumers are being deprived of various after sales rights such as the rights of withdrawal and warranty rights (see par. 2.4) as they no longer have the means to contact the trader and invoke their rights. This is especially concerning when the trader, after causing many problems, continues its commercial practices elsewhere. As a result, the practice of disappearing web shops often generates consumer complaints to the CPC Authorities and the network of European Consumer Centres (ECC-NET). The easy-removal option for websites facilitates or even encourages non-compliance with the legal requirements of professional diligence for online traders and it facilitates rogue traders that choose to use hit-and-run tactics by continuously operating new websites for a brief period, misleading consumers and then removing the website when complaints become too numerous to subsequently start a new website.

When a Shopify web shop gets deactivated, it should at least still mention the basic company identification and contact details for consumers for a reasonable period (e.g. at least 6 months after deactivation) to ensure that consumers can effectively exercise their rights.

Legal framework:

- Directive 2000/31/EC on electronic commerce
  - Article 5(1)(a-g)
- Directive 2005/29/EC on unfair commercial practices
  - Article 5
  - Article 7(1), (2), (4)(b)
- Directive 2011/83/EU on consumer rights
  - Article 6(1)(b) and (c)

2.2. Fake discounts, delivery issues and additional hidden costs

CPC authorities noticed Shopify web shops that became active only recently, while the trader already heralds great product discounts. If a trader has never practiced the reference price before, this is a misleading commercial practice. Similarly, traders cannot present a price as a discounted price, when in fact the reference price has never been truly carried.

Also, the trader needs to inform the consumer correctly on the delivery timing and, in case delivery will not be done by the web shop itself, that a third party located outside the EU will deliver the product. CPC authorities noticed these drop shipping web shops often do not contain correct information on the delivery timing and delivery by a third party. Some web shops even contain misleading mentions like “bought today, sent today”. However, *in casu* the goods were sent from

China and it took more than a month for the consumer to receive them, while the consumer estimated a quick delivery.

Furthermore, many traders do not properly inform consumers prior to their purchase that additional costs associated with the import of products into the EU might be incurred by the consumer.

Legal framework:

- Directive 2005/29/EC on unfair commercial practices
  - Article 6(1)(b) and (d)
- Directive 2011/83/EU on consumer rights
  - Article 18

2.3. Dark patterns: unfair commercial practices

Moreover, CPC authorities noticed Shopify web shops that raise concerns regarding various unfair commercial practices, e.g.:

- fake scarcity claims: web shops containing fake limited stock notices, e.g. "only [x] items left";
- pressure selling: fake countdown timers for a limited time offer (but when the countdown timer expires, it starts counting down again);
- social proof: fake social proof pop-ups, e.g. "[x] people bought this product today", while a trader has the option to modify this number into a fake one using a plug-in.

All statements should be clear and accurate so that consumers are not misled as to the popularity and availability of a product. Any specific limitation or defining criteria, which apply to popularity or availability statements, should be stated upfront in a prominent manner and should be clearly disclosed. Online tools, plug-ins or other software based solutions that generate random messages directed at consumers, such as randomised scarcity claims, repeating count down clocks or fabricated reviews, constitute per se violations of EU consumer legislation.

Legal framework:

- Directive 2005/29/EC on unfair commercial practices
  - Article 5
  - Article 6 (1)(a) and (b)
  - Article 7(2)
  - Article 8
  - Annex I, several practices, e.g. no. 7

2.4. Consumer rights: right of withdrawal and consumer guarantees

Web shops need to provide the consumer information regarding his basic consumer rights such as the right of withdrawal (14 days) and the legal guarantee of conformity for goods. This needs to be done upfront in a clear and comprehensible manner. CPC authorities noticed Shopify web shops lacking this mandatory information. Especially when the product needs to be returned to an overseas supplier, the web shops need to clearly state the costs involved with returning products in case of the exercise of the right of withdrawal, since the situation will be different from what the consumer will expect. In the case of a faulty product and the use of warranty rights, the web shop is legally required to guarantee free replacement of the product or a refund for the consumer. This includes a free-of-charge possibility to return the product to the web shop (not the manufacturer).

Especially regarding traders using drop shipping, CPC authorities also received consumer complaints stating that their web shops told the consumer, after receiving the goods, to settle any issues regarding the goods with the third party supplier, often located in China, as the trader itself does not handle the goods. Such a statement is in clear violation of the trader's responsibilities in EU consumer law.

Legal framework:

- Directive 2011/83/EU on consumer rights
  - Article 6(1)(h-l)
- Directive 1999/44/EC on certain aspects of the sale of consumer goods and associated guarantees

2.5. Scams, counterfeit and product safety

A final, but most worrying aspect are consumer reports regarding scams, the sale of counterfeit and products with product safety concerns (such as the lack of product safety certification). At first, during the Covid-19 crisis, CPC authorities noticed scams related to Covid-19 health products. Then, there was a gradual shift towards more general no delivery scams or scams where consumers receive a different product of lower value than the one they ordered (e.g. receiving a skipping rope when ordering advanced fitness equipment or receiving a window sticker when ordering a decorated Christmas tree including a moving train). This way, the fraudulent trader can fend off any claims saying a tracking code of the shipment exists (the consumer does receive the goods, but not the ones he ordered) and when the web shop is subsequently taken down by the trader after a short social media campaign, the consumer only has the order confirmation emails which only contain a vague description of the product ordered (e.g. "fitness tool" or "Christmas tree") so he cannot prove he received another product of lower value. Even if a consumer can prove non-conformity, this will not help since the web shop is likely to be inactive and can no longer be contacted by the consumer.

Again, making sure company identification details are clearly provided on each web shop is a basic legal obligation to protect consumers against scam practices, together with a quick and efficient notice & takedown procedure (see par. 3.2). Furthermore, we invite Shopify to explain what steps it takes to verify (new) customers and to explain the "vetting process" or any (periodic) audits it undertakes to combat fraud.

Legal framework:

- Directive 2005/29/EC on unfair commercial practices
  - Article 5
  - Article 6 (1)(a) and (b)
  - Article 7(2)
  - Article 8
  - Annex I, no. 9

2.6. Drop shipping and operations by minors

Most Shopify web shops that generate consumer complaints are using drop shipping. The trader has no physical stock of the goods he sells, but instead he transfers the orders to a third-party supplier. The third-party supplier then directly delivers the goods to the consumer. As the trader does not handle the goods, he has little or no direct control over products and their shipping. The trader only chooses the products he will sell and handles the direct sales and marketing.

Shopify offers the Oberlo app to traders to quickly add products to their Shopify web shop using drop shipping from e.g. AliExpress. According to an analysis of the Netherlands Authority for Consumers and Markets, around 80% of the web shops that use drop shipping, and that cause consumer issues on the Dutch market, are Shopify web shops.

CPC authorities also observe that some (former) drop shipping traders that are or were active through Shopify organise paid training sessions for prospect drop shippers. These "drop ship academies" often overstate the potential gains and understate the risks and responsibilities connected with operating a drop ship business. Often, they also promote the use of unfair commercial practices to achieve the potential high gains they promise. As those practices are in high risk of misleading consumers, they should not be encouraged supported, incentivised or facilitated by Shopify.

Additionally, those practices are often targeted at young adults and minors, who are less aware of risks and therefore vulnerable. The Netherlands Authority for Consumers and markets is under the impression that also minors operate websites on the Shopify platform. The limitations on minors to conduct legally binding actions might affect consumer rights. We invite Shopify to clarify whether under its terms and conditions it excludes minors from operating web shops and, if yes, to explain the measures it takes to properly check the age of users and to prevent minors from being able to operate web shops on its platform.

3. Cooperation with CPC authorities

3.1. Legal analysis

3.1.1. EU establishment

Even though Shopify is headquartered in Canada, according to its Terms of Service (article 3(a-b) of https://www.shopify.com/legal/terms), if the trader's billing address is in Europe, then the "Shopify Contracting Party" will be Shopify International Limited, a private company limited by shares, incorporated in Ireland. In this case, the trader is automatically subjected to the jurisdiction of the Irish courts.

Recital 19 of the e-Commerce Directive (Directive 2000/31/EC)[6] provides for some details, also based on case-law: *"the concept of establishment involves the actual pursuit of an economic activity through a fixed establishment for an indefinite period; the place of establishment of a company providing services via an Internet website is […] the place where it pursues its economic activity; in cases where a provider has several places of establishment it is important to determine from which place of establishment the service concerned is provided; in cases where it is difficult to determine from which of several places of establishment a given service is provided, this is the place where the provider has the centre of his activities relating to this particular service"*.

From the company's Terms of Service, it is clear that traders established in the EU enter in an intermediation contract with Shopify International Limited, established in Ireland.

[6] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')

3.1.2. Provider of information society services

As highlighted by the Court of Justice of the European Union (CJEU), in case C-324/09 "L'Oréal v. eBay"[7]: "*an internet service consisting in facilitating relations between sellers and buyers of goods is, in principle, a service for the purposes of Directive 2000/31. That directive concerns, as its title suggests, 'information society services, in particular electronic commerce'. It is apparent from the definition of 'information society service', cited at paragraphs 8 and 9 of this judgment, that that concept encompasses services provided at a distance by means of electronic equipment for the processing and storage of data, at the individual request of a recipient of services and, normally, for remuneration. It is clear that the operation of an online marketplace can bring all those elements into play.*"

As hosting third-party content, Shopify is a provider of information society services that consists of the storage of information provided by a recipient of the service. Furthermore, its obligations and liability as a hosting service are regulated by Article 14 of the e-Commerce Directive.

3.2. Notice & action procedure: provide an email address and cooperate with CPC authorities

As an information society service provider, Shopify is required by EU legislation, and in particular Article 5(1)(c) of the e-Commerce Directive, to make easily and permanently accessible to the recipient of the service and to national competent authorities and/or designated bodies within the meaning of the CPC regulation, adequate contact information, including an email address, so that they can be "*contacted rapidly and communicated with in a direct and effective manner*".

This requirement is in the interests of fair trading in electronic communications, as it provides consumer protection authorities with means to rapidly signal any practices which may infringe consumer or other legislation.

It is also in the interest of Shopify to establish effective cooperation mechanisms with enforcement bodies to help keep their web shop ecosystem safe and trustworthy for consumers and to keep it free from the risks posed by illegal commercial practices, which may harm consumers, and especially vulnerable groups.

Recital 40 of the e-Commerce Directive further clarifies that "*service providers have a duty to act with a view to preventing or stopping illegal activities*". Based on Article 14 of the same Directive, information society service providers, which act as hosting services are not liable for the information stored by their users when they have no actual knowledge of illegal activities or content. However, Article 14(1)(b) requires that "*the provider upon obtaining knowledge or awareness [of illegal activity or information], acts expeditiously to remove or disable access to the information*". Article 14(3) further clarifies this Article shall not affect the possibility for an administrative authority "*of requiring the service provider to terminate or prevent an infringement*".

[7] C-324/09 Judgment of the Court (Grand Chamber) of 12 July 2011, L'Oréal SA and Others v eBay International AG and Others

In view of these requirements, CPC authorities may require the cooperation of Shopify, acting as a hosting service provider, in providing them a dedicated email address so that it can be contacted in case they have found content or practices which are likely to breach consumer legislation and in particular Directive 2000/31/EC on electronic commerce, Directive 2005/29/EC on Unfair Commercial Practices, Directive 2011/83/EU on Consumer Rights, Directive 93/13/EC on Unfair Contract Terms and Directive 1999/44/EC on the Sale of Goods and Associated Guarantees.

As mentioned above, in the past months, CPC authorities have acquired evidence that a number of practices in breach of these Directives are taking place on Shopify web shops such as:
- web shops directed towards European consumers with no company identification;
- misleading pre-contractual information, for example where the identity and the details of the trader, the price, availability or main characteristics of products are not provided or are inaccurate;
- use of dark patterns (e.g. pressure selling);
- marketing of counterfeited products or (Covid-19) products with product safety issues; and
- (Covid-19) scams involving payments taken from consumers.

To make the exchange of information efficient and mutually beneficial between consumer authorities and Shopify, CPC authorities propose to establish a standardised communication format which will include the following elements:

From Competent Authorities[8]:
- Description of the content deemed illegal (with screenshots when available);
- Description of reasons and legal bases (including references to the relevant provisions in the EU consumer Directives and their national transposition measures);
- Description of the action requested by the authority:
    - to obtain from Shopify information about the trader that owns the web shop so that this trader can be efficiently contacted;
    - and, in case the content is likely to cause harm to consumers (such as scams or the lack of basic company identification), the immediate taking down of the content until further notice.
- If needed, further justification of the issue at stake.

From Shopify
- Acknowledgement of receipt of the request;
- Provision of the information requested and of any other relevant information;
- In case of a request for taking down the content, information on the action taken and, if no action is taken, the legal and factual reasons for this.

Timeline
The procedure should contain deadlines for the various exchange of information so as to address the issues raised by illegal content rapidly. The possible suggested deadlines could be the following: [1] day for acknowledgement of receipt, [3] days for request to provide information and/or take down content and report on this, or provide reasons for not taking down content.

National Procedures

[8] In addition to Competent Authorities, relevant entities include Single Liaison Offices and designated bodies within the meaning of the CPC Regulation.

This proposed CPC procedure is intended to facilitate efficient cooperation between Shopify and national enforcers. It does not pre-empt national authorities from using other procedures and enforcement measures (e.g. official requests for information or action) as it is appropriate in order to ensure compliance with national law.

Legal framework:

- Directive 2000/31/EC on electronic commerce
  - Recital 40
  - Article 5(1)(c)
  - Article 14(1)(b)
  - Article 14(3)

3.3. Identification of web shops: respect minimum investigation powers of CPC authorities

Under the Consumer Protection Cooperation (CPC) Regulation (EU) 2017/2394, Member State authorities have certain minimum investigation powers (article 9). As noted above, Member State authorities have the power to ask the identification of a trader as part of their "*power to require any […] legal person to provide any relevant information, data or documents, in any form or format and irrespective of their storage medium, or the place where they are stored, for the purposes of establishing whether an infringement covered by this Regulation has occurred or is occurring, and for the purposes of establishing the details of such infringement, including tracing financial and data flows,* ***ascertaining the identity of persons involved*** *in financial and data flows, and ascertaining bank account information and* ***ownership of websites***" (article 9(3)(b)).

After ascertaining the identity of the trader and the persons involved, CPC Authorities can use this information to send requests for enforcement measures to other Member States (article 12) if the trader is located in another Member State.

As such, Shopify is required by EU law to provide CPC authorities on request with trader identifications of European Shopify web shops and web shops directed towards European consumers.

Legal framework:

- Regulation (EU) 2017/2394 on cooperation between national authorities responsible for the enforcement of consumer protection laws
  - Article 9(3)(b)