



Republika ng Pilipinas
KAGAWARAN NG KATARUNGAN
Department of Justice
Manila

OFFICE OF CYBERCRIME
ADVISORY OPINION NO. 02 (Series of 2015)
30 April 2015

ADVISORY ON ONLINE SHOPPING FRAUD

INTRODUCTION

This Advisory is issued to inform online shoppers of the risks involved in dealing online, as well as to guide online shopping providers in providing a safe and secure online shopping environment, in the promotion of consumer welfare.

Online shopping started to thrive following technological advances and the prevalent use of the internet. As it provides a fast and convenient way for consumers to purchase goods and services, it is becoming the preferred method of purchasing and has popularized online shopping platforms such as Lazada, OLX, Hallo Hallo, Metrodeal, Beconomic (Groupon).

Risks, trade malpractices, and operational challenges exist in online shopping in view of the anonymity being offered by the internet. Issues, such as the following, make it important for online shoppers to take necessary precautions to protect themselves when shopping online:

- Frauds and scams;
- Misleading or deceptive product advertisements;
- Difficulty in returns and replacements;
- Unexpected customs dues, transaction costs, and surcharges;
- Privacy breaches and abuse of user information; and
- Chaotic delivery procedures.

SUMMARY OF APPLICABLE LAWS

It is the policy of the State to protect the interests of the consumer, promote his general welfare, and guard against deceptive or unfair business practices, as it recognizes the vital role of

information and communications technology, and the importance of an online environment conducive to social and economic development.

Republic Act No. 10175 or the “Cybercrime Prevention Act of 2012” (R.A. 10175), which aims to regulate access to and use of the cyberspace, provides that *“all crimes defined and penalized by the Revised Penal Code, as amended, and special laws, **if committed by, through and with the use of information and communications technologies** shall be covered by the relevant provisions of this Act: Provided, That the penalty to be imposed shall be one (1) degree higher than that provided for by the Revised Penal Code, as amended, and special laws, as the case may be.”* (Emphasis supplied)

Republic Act No. 7394 or the “Consumer Act of the Philippines” (R.A. 7394) advances the *“protection against deceptive, unfair and conscionable sales acts and practices”* as well as promotes the *“provision of information and education to facilitate sound choice and the proper exercise of rights by the consumer.”*

Further, Republic Act No. 8792 or the “Electronic Commerce Act of 2000” (R.A. 8792), which aims to facilitate the dealings, transactions, arrangements agreements, contracts and exchanges and storage of information through the utilization of electronic medium, extends the coverage of Republic Act No. 7394 or the “Consumer Act of the Philippines” to transactions made with the use of electronic medium.

Through the Joint Department of Trade and Industry (DTI)–Department of Health (DOH)–Department of Agriculture (DA) Administrative Order No. 01, Series of 2008 (Joint Administrative Order No. 01), “Online Shopping” is included in the coverage of R.A. 7394, classified as transactions through electronic means under R.A. 8792.

Difference, however, between a *seller* in its normal sense and a *seller* contemplated under Article 4 (bn) of RA 7394 should be made.

RA 7394 provides:

“Art. 4. Definition of Terms.

x x x

(bn) "Seller" means a person **engaged in the business** of selling consumer products directly to consumers. It shall include a supplier or distributor if (1) the seller is a subsidiary or affiliate of the supplier or distributor; (2) the seller interchanges personnel or maintains common or overlapping officers or directors with the supplier or distributor; or (3) the supplier or distributor provides or exercises supervision, direction or control over the selling practices of the seller.

x x x" (Emphasis supplied)

For a person to be considered as a *seller* under R.A. 7394, he should be **engaged in the business** of selling consumer products directly to consumers.

If a *seller*, in its normal sense, is an individual or a group of individuals not registered with the Securities and Exchange Commission (SEC) or the Department of Trade and Industry (DTI), the applicable law is Article 315 (Swindling/Estafa) of the Revised Penal Code.

On the other hand, if a *seller* falls under the definition provided by R.A. 7394 - a registered entity with the SEC or DTI - then the applicable law is the Consumer Act of the Philippines.

Both laws, however, can be related to R.A. 10175 if committed by, through and with the use of information and communications technologies.

The following are laws and related issuances to regulate "sellers" as defined in R.A. 7394:

DECEPTIVE SALES PRACTICES

Article 50 of the Consumer Act considers practices as "deceptive" "*whenever the producer, manufacturer, supplier or seller, through concealment, false representation of fraudulent manipulation, induces a consumer to enter into a sales or lease transaction of any consumer product or service.*" The following representations of sellers or suppliers are deceptive sales practices, which are prevalent today:

- (a) *a consumer product or service has the sponsorship, approval, performance, characteristics, ingredients, accessories, uses, or benefits it does not have;*

One common trick is to present a product in a photograph “for illustrative purposes” when the actual item description does not include such accessories or parts, or has extra costs in the inclusion of such parts.

In SLR and DSLR cameras, the body and lens are often sold separately, but “body-only” sets are commonly understood to include basic parts such as batteries, a charger, a memory card, and the like. However, the “body-only” clause are often interpreted strictly in a bait-and-switch scheme to upsell basic parts after deposit of payment.

There is also a scheme where products are advertised to have slimming or health benefits that cure cancer and other medical conditions. Such products are rarely properly tested and can even be harmful.

- (b) *a consumer product or service is of a particular standard, quality, grade, style, or model when in fact it is not;*

Technological goods upgrade models frequently, and sometimes, older models do not look significantly different to the newer ones. Especially when the updated model name is similar to the older version, some vendors can include descriptions and photographs of the new model when the actual specifications reflect the older one.

- (c) *a consumer product is new, original or unused, when in fact, it is in a deteriorated, altered, reconditioned, reclaimed or second-hand state;*

Another common trick is to present a brand-new packaged item in the product ad, but upon confirmation of the order, the supplier replaces the contents of the brand-new packaging with a refurbished or second-hand model, re-seals it, and then ships it to the unsuspecting customer.

- (d) *a consumer product or service can be supplied in a quantity greater than the supplier intends;*

For Daily Deals or Group-Buying sites, companies provide heavily discounted promotions for a set time limit or a set quantity. Very good deals under a time limit can sometimes attract a huge wave of customers that the suppliers did not anticipate.

In these cases, the supplier sometimes does not have enough actual capacity to service the amount of deals transacted. This can lead to a huge backlog, where sometimes the length of delay is indefinite. In other cases, the supplier will try to switch out certain provisions of the deal and hope the customer goes along with it.

- (e) *a **specific price advantage** of a consumer product **exists when in fact it does not**;*

Some online vendors advertise their product as cheaper than a posted Suggested Retail Price (SRP), when in fact, no SRP exists for that product, or the posted SRP is inaccurate. In other cases, a promotion will present a discounted price against a stated original price, though the “original price” has been artificially increased to make the discount seem impressive.

- (f) *the sales act or practice involves or **does not involve a warranty**, a disclaimer of warranties, particular warranty terms or other rights, **remedies or obligations if the indication is false**; and*

Many online vendors, often unregistered, do not offer any warranty or exchange policy. Many customers do not realize that the cheaper prices are due to the lack of warranty. Warranties may also be advertised, but have several challenges, such as: no clear identification or instruction or claiming the warranty, undue restrictions, small time windows, or uncooperative behavior in servicing the warranty.

CLEAR, IDENTIFIABLE CREDENTIALS AS REQUIRED BY LAW

To reduce the risk of fraud in online markets, Section 5 of Joint Administrative Order No. 01 requires retailers, sellers, and suppliers engaged in electronic commerce to provide accurate, clear and accessible identification of the following:

1. Department of Trade and Industry (DTI) and/or Securities and Exchange Commission (SEC) registration;
2. Name of the owner/proprietor of a retail establishment in case of a single proprietorship and names of directors and other officers in case of a corporation;
3. Principal geographical address of the retailer, seller, distributor, supplier or manufacturer, and when applicable, of offices or agents in the Philippines;
4. Website, e-mail address or other electronic means of contact, telephone and fax numbers of the retailer, and when applicable, of its offices or agents in the Philippines;
5. Any relevant local or foreign government registration/license numbers such as but not limited to the local government unit's permit to operate, Taxpayer's Identification Number (TIN), when applicable;
6. Contact details about any business association or organization membership, when applicable; and
7. Representative Agent/s in the Philippines for purposes of summons.

TRANSPARENCY ON PAYMENT, CHARGES, AND DUES

In many cases, customers are surprised by additional costs such as when the price tag do no not include surcharges, or when a "cheap" imported product do not disclose additional payment of customs dues.

Section 5 of Joint Order 01 thus requires online merchants to provide **"sufficient, clear, accurate, easily accessible information about the terms, conditions and costs of the consumer transaction. The required information includes applicable costs not part of the price tag itself, such as *delivery*, postage, handling, *insurance*, shipping charges, *taxes*, and specific reference to any other charges, *customs fees* and other fees that may be imposed on or collected from consumers."**

In addition, online sellers are responsible for informing the customer on *"available methods of payment, the security of those payment methods in clear, simple language, how to cancel regular payments under those methods, and any costs applicable to those payment methods."*

DATA PRIVACY

Another concern in online shopping is the security of personal data. Many consumers disclose sensitive information such as credit card details, bank accounts, and passwords, unaware that it can be intercepted and used for illegal purposes such as identity theft, credit card fraud, or sale of personal information, which is punishable under the R.A. 10173 or the "Data Privacy Act."

DTI Administrative Order No. 8, Series of 2006 or "Prescribing Guidelines for the Protection of Personal Data in Information and Communications Systems in the Private Sector", contains instructions on the protection of personal data, what constitutes lawful access to personal data, obligation of confidentiality, and requirements for mechanisms ensuring security of data, which any retailer engaged in the business of electronic commerce is required to comply with.

Consumers using any online medium for e-commerce should be informed (1) whether or not their personal information are being processed or are to be processed; (2) purposes of processing said information; (3) a description of the personal information being used; and (4) the recipients or classes of recipients to whom they are or may be disclosed.

Consumers also have the right to request rectification, destruction of his personal data, restriction of further processing of his personal data, and object to the processing of his or her personal data if it would be used for commercial purposes.

In any case, the online retailer (data processor) may only process personal data entrusted to him or her only within the scope determined in the contract and in accordance with the purposes provided for therein. The online retailer is obligated to delete or block the personal data once the intended purpose is achieved. Thus, consumers must take care to read privacy policies in detail before agreeing to them.

ADVISORY

In view of the foregoing, the following points are stated:

1. "PREVENTION IS BETTER THAN THE CURE"

Consumers must remain vigilant and proactive in protecting their welfare and rights. Like traditional markets, customers should keep in mind the principle of *caveat emptor* (buyer beware) in their online dealings. It is highly important to be wary of online fraud to avoid the arduous process and inconvenience of recovering any damage.

Below are some tips on how to protect yourself from online shopping fraud:

How to protect yourself from online shopping fraud:

DO's

- ✓ Keep security software and firewalls up-to-date.
- ✓ Update your internet browser as and when a new patch is released.
- ✓ Research a seller before making an online purchase. Independently verify their contact details and other company information.
- ✓ Invest the time to read all details of an offer to sell.
- ✓ Be wary of unsolicited emails from online businesses that you do not know.
- ✓ Use strong passwords, which contain a combination of letters, numbers and other characters. Change them regularly and use different passwords for different online accounts.
- ✓ Read and understand the seller's terms and conditions and privacy policies.

DON'Ts

- Shop online using public computers if you can avoid it.
- Access websites via links embedded in emails. Type the website address into the browser yourself.
- Respond to unsolicited emails from people or businesses you don't know. Delete them.
- Divulge personal or financial information and passwords to anyone requesting them by email.
- Use the same password for all your online accounts and websites.
- Use 'easy' passwords (such as any word from a dictionary).
- Disclose personal or credit card information on a website unless it is secure.
- Believe everything you read – if it sounds too good to be true, it probably is false!

- ✓ Check that a green padlock symbol is displayed either in the bottom right-hand corner of the webpage or in the address bar and verify the same.
- ✓ Be vigilant in transmitting financial and personal information. Avoid unsecure channels like public Wi-fi, email, phone calls, or mobile messaging.

The “Red Flags”

Be mindful of some of the “red flags” of an online shopping fraud:

- Products are advertised at very low prices compared to other websites – if it sounds too good to be true, then it probably is a fraud!
- Online sellers with poor ratings and/or feedback.
- Online sellers who ask you to pay by money transfer service or direct to their bank account rather than through the site’s preferred payment method.
- Websites with no contact details such as a physical address or telephone number.
- Websites with limited or no information about privacy and their terms and conditions of use.

Steps to take before you purchase online

Make sure your online purchases are secure by taking some simple precautions:

- **Protect your computer:** Keep security software such as anti-virus and anti-spyware up-to-date. Update your browser regularly. Exercise caution when using public computers to make online purchases.
- **Research the seller:** Check online reviews and customer feedback to find out if the individual and/or business are reputable.

- **Know the terms of the sale:** Check the terms and conditions of the transaction, warranties, policies on refunds and replacements, mechanisms for addressing buyer complaints, and the costs or other additional charges to the item price.
- **Use strong passwords:** Use strong passwords when setting up online accounts. Passwords should contain a combination of letters, numbers and other characters. Change them regularly and use different passwords for different accounts.
- **Know your rights:** Read and understand the business's terms and conditions and privacy policies before you sign-up or make a purchase.
- **Review website security:** When you proceed to checkout, make sure that a padlock symbol is displayed in either the bottom right-hand corner of the webpage or in the address bar. Click the padlock to make sure the security certificate is valid. The website address should begin with 'https'.
- **Take extra precautions for online shopping websites:** Do not make payments directly to a seller's bank account – regardless of the reasons given. Use the auction website's preferred payment methods to ensure access to their disputes resolution processes. Another good option is to have Cash-on-Delivery terms.
- **Keep a record:** Keep a record of your online purchases. Regularly monitor your bank, credit card, and store card statements for any unusual transactions.

2. SEEK ASSISTANCE AND REDRESS FROM RELEVANT REGULATORY AGENCIES.

Consumers must be aware that they are entitled to the same consumer rights online as they are offline. These rights include the right to demand a refund or replacement, the right to be duly informed of all pertinent information and costs, the right against

illegal use of their personal data, and the right against deceptive trade practices.

The presence of internal mechanisms that address consumer complaints do not prevent a buyer from seeking redress from legal authorities.

In the event of inconsistency or inconformity with the provisions of our laws, the public are encouraged to provide their feedback or file their complaints to the appropriate government agencies, which are the following:

For matters involving the sale of food, drugs, cosmetics, health devices and hazardous substances, consumers may contact the Department of Health Food and Drug Administration Office at (02) 857-1986 to 99.

For matters involving the sale of agricultural, primary and secondary processed goods such as fertilizer, feeds, and the like, consumers may contact the Department of Agriculture Agribusiness and Marketing Assistance Office at (02) 920-2216.

For matters involving “sellers” registered with the DTI or SEC, consumers may contact the DTI through its Consumer Welfare Desk at 811-8231 (Metro Manila) or (02) 751-3330 (outside Metro Manila), or the SEC through its Public Information and Assistance Hotline at 584-1119.

For matters involving online fraud, consumers may contact the following: the PNP – Anti-Cybercrime Group at (02) 723-0401 local 5313, the NBI – Cybercrime Division at (02) 523-8231 local 3455, or the DOJ – Office of Cybercrime at (02) 523-8481 local 222.


Consumers are also encouraged to secure copies of electronic messages or documents related to the transaction, as these are considered authentic and reliable in facilitating dealings, transactions, and agreements, and may be used as evidence against the fraudster.

3. BEWARE OF OTHER TYPES OF ONLINE FRAUD.

Online fraud is not limited to online shopping. Internet users should also be wary of the following types of online fraud that are punishable under the Cybercrime Prevention Act:

- **Fake websites:** A website that either mimics a genuine reputable online business by using a very similar website address or that pretends to be a legitimate business with the sole purpose of defrauding unsuspecting shoppers.
- **Online auction scams:** Receiving goods that are counterfeit or that significantly differ from the original description and are of lesser value. In some cases, no goods were delivered at all. The fraudster may also try to persuade his victim to pay by means other than the preferred method of the auction website.
- **Weight loss or medicine scams:** A scheme which offers alternative slimming aids or medicines to cure obesity, cancer and other medical conditions. These products are rarely properly tested and can even be harmful.
- **Phishing emails:** Emails purportedly received from a legitimate and well-known source which contains a link to a false but credible-looking website where the victim will be asked to update their personal and/or account information. Note: banks and other legitimate online businesses will not ask you to do this.

This Advisory is issued by the DOJ-OOC in line with its mandate to educate the public and ensure that the near limitless potential of cyberspace is safeguarded from malicious individuals, and from the abusive, fraudulent, or harmful corrupt business practices as well. All are hereby enjoined to disseminate and faithfully observe this Advisory.


LEILA M. DE LIMA
Secretary

Department of Justice
CN : 0201504723



8