COMPETITION AND CONSUMER PROTECTION COMMISSION

CONSUMER PROTECTION DEPARTMENT

Consumer Financial Education Strategies on How to Identify and Combat Online Scams - CCPC-Zambia

Introduction

The Commission is currently brainstorming various initiatives that could be used to effectively raise awareness, enhance productivity, case initiation and more efficient ways of curbing contraventions of the Competition and Consumer Protection Act No. 24. Of 2010 (CCPA).

This paper seeks to discuss various types of Online Scams, Proactive/Preventive Measures thereof, Indicators by which to identify such Scams as well as the Various Strategies which the Commission may endeavor to use in raising awareness to the members of the public.

NB: ***The write up below is not exhaustive and includes initiatives already employed by the Commission which may require strengthening or re-strategizing, new initiatives that may require exploring and will require input from all staff in the department for effective implementation during the Covid-19 pandemic and beyond.***

Discussion

Types of Online Scams:

A scam is a deceptive scheme or trick used to cheat someone out of something, especially money.[1] Therefore, an Online Scam/Internet Fraud is a type of cybercrime fraud or deception which makes use of the Internet and could involve hiding of information or providing incorrect information for the purpose of tricking victims out of money, property, and inheritance. It may also include theft of personal information or identity theft.

There are various forms of online scams which may include among others, the following; and may border on; **Money & Credit; Home loans & Mortgages; and Jobs & Money Making:**

[1] www.dictionary.com *accessed on 3/02/2021, 13:42*

Money and Credit types of Scams

- **Identity Theft**

Identity (ID) Theft occurs when a party acquires, transfers, possesses, or uses personal information of a natural or legal person in an unauthorised manner, with the intent to commit, or in connection with, fraud or other crimes. Although this definition encompasses both individuals and legal entities, focus in the present guidance is limited to identity theft affecting consumers. Traditionally, ID theft is committed by accessing information acquired from public records, theft of personal belongings, improper use of databases, credit cards, and chequing and saving accounts and misusing that information. Unauthorised access to personal data can be carried out by various means, including *dumpster diving*, *payment card theft*, p*retexting*, *shoulder surfing*, *skimming,* or *business record theft*. (OECD POLICY GUIDANCE ON ONLINE IDENTITY THEFT –3 © OECD. Box 1).

- **Phishing**

Phishing is a method that thieves use to lure unsuspecting Internet users' personal identifying information through emails and mirror-websites which look like those coming from legitimate businesses, such as financial institutions or government agencies. Typically, a phishing attack is composed of the following steps:

The phisher sends its potential victim an e-mail that appears to be from an existing company. - *The e-mail uses the colours, graphics, logos, and wording of the company. - The potential victim reads the e-mail and provides the phisher with personal information by either responding to the e-mail or clicking on a link and providing the information via a form on a website that appears to be from the company in question. - Through this, the victim's personal information is directly transmitted to the scammer.*

- **ATM Fraud**

Is a form of fraud where ATM cards may be cloned after obtaining consumer details fraudulently.

Proactive/Preventive Measures

Keep Your Personal Information to Yourself - Protect your passwords, guard your credit card number, shred sensitive paperwork, and do not leave your mail where it might tempt a potential identity thief.

Socialize safely online **-** When using social networking sites update your privacy settings to restrict access to people you trust. Post only information you are comfortable with the whole world knowing, because once it is posted, you can't take it back. Do not post your Social Security number, your national registration card number, ATM cards or financial information. Use caution when sharing details about where you work, where you hang out, and what is going on with you and your friends.

P2P File-Sharing can be risky - Peer-to-peer file-sharing can open the door to unwanted content, spyware, and viruses. If you decide to use file-sharing software, install it carefully. Otherwise, you might give strangers access not just to the files you intended to share, but also to other information on your hard drive, like email and personal documents.

Travel Scams Turn Summer Breaks into Summer Busts. Be aware that scam artists target people who are looking for low-cost vacations. Before you show up at the airport/ or intended camp, carefully review any promotional materials before consenting to making a payment as well as filling necessary forms. Also review the tour package carefully and investigate the operator.

Phishing Scams Roll in Personal Information. Perhaps at some point in time you may have received emails claiming to be from your bank asking you to "verify" your credit card or checking account number. They are from fraudsters phishing for your information. Never give out your personal information in response to an email. When in doubt, check it out by calling the company directly. Ensure you delete suspicious emails in your junk or spam folders.

Consumer Education

Educate yourself on the importance of changing passwords regularly to avoid scammers' access to your personal information in instances where your accounts have been hacked. Also log out successfully after making online transactions.

Home Loans and Mortgage types of Scams

Information is critical when you are shopping for a mortgage. It is equally important to know the consequences of falling behind on your payments and the tell-tale signs of a foreclosure rescue scam.

Deceptive Mortgage Adverts

Some adverts for mortgages promise more than they can deliver. You may see or hear ads with offers of low rates or payments. Whether you see them on the Internet, on television or in the paper, or whether they come by fax or mail, some of these ads look like they are from your mortgage company or a government agency. Regardless of where you see the ads, remember that while the offers are tempting, some are terribly flawed: they do not disclose the true terms of the deal as the law may require.

Indicators of a Possible Mortgage Scam

Words that should trigger follow-up questions, as well as information to insist on after you've read an ad may include the following;

A Low "Fixed" Rate - Ads that tout a "fixed" rate may not tell you how long it will be "fixed." The rate may be fixed for an introductory period only, and that can be

as short as 30 days. When you shop for a mortgage, you need to know when and how your rate, and payments, can change.

Very Low Payment Amounts - Ads quoting a very low payment amount probably aren't telling the whole story. For example, the offer might be for an Interest Only (I/O) loan, where you pay only the amount of interest accrued each month. While the low payment amount may be tempting, eventually, you will have to pay off the principal. Your payment may go up after an introductory period, so that you would be paying down some of the principal – or you may end up owing a "balloon" payment, a lump sum usually due at the end of a loan.

Teaser Rates - Ads with "teaser" short term rates or payments don't often disclose that a rate or payment is for a very short introductory period. If you don't nail down the details in advance about your rates and payments for every month of the life of your loan, expect payment shock when the rate and payment increase dramatically.

Monthly Interest rates as opposed to yearly rates - The rates quoted by lenders are annual rates. On most home mortgages, the interest payment is calculated monthly. Hence, the rate is divided by 12 before calculating the payment.

Other fees such as administrative fees not well defined - Loan Administration Fee means a fee charged by a Lender in consideration of administrative costs and expenses incurred by the Lender in connection with each commitment advance of the loan, these need to well defined/explained to you.

Flexible interest rates and fixed interest rates - A fixed-rate mortgage charges a set rate of interest that does not change throughout the life of the loan while a flexible interest rate changes with economic indicators.

Jobs and Money-Making types of Scams

There are some mighty convincing promoters out there who promise high returns, low risk, and 'golden' opportunities just waiting for the right buyer. Take the time to ask the questions that can keep you from getting ripped off. Offers that promise quick and easy income from doing some activity at home virtually never pay off; For example;

Facebook, Email, Twitter, Instagram, WhatsApp and/ or Envelope-Stuffing Scheme - Ads for "opportunities" can be anywhere — from your mailbox to your inbox, in the newspaper or on an online search. Promoters usually advertise that for a "small" fee, they will tell you how to earn big money doing a particular activity at home. They may say you will earn money for each activity, it could be sharing their page, reading their blog or anything, making it possible for you to earn hundreds or even thousands of Kwacha. They promise to send you money but they really do not, hence one loses out the money (a small fee) they sent earlier.

Ponzi Schemes

What happens is that once you send your money, you're likely to get feedback telling you to get other people, even your friends and relatives, to buy the same envelope-stuffing "opportunity" or another product. The only way you can earn money is if people respond to your solicitations the same way you responded. The promoters rarely pay anyone.

Fake Corporate Social Media Pages

There is a growing trend by scammers to impersonate small and medium enterprises with intent to scam unsuspecting members of the public. Scammers can use social networks to gain your trust by passing for official profiles. By pretending to be from customer service or sharing a fake deal, they can reach groups all at once or target individuals to swindle them.

INDICATORS OF A POSSIBLE SCAM

Recognizing these Four (4) common signs of a scam could help Consumers avoid falling for one;

Scammers "PRETEND" to be from an organization you know.
Scammers often pretend to be contacting you on behalf of some reputable organisation/government. They might use a real name, like the ZRA, NAPSA, ZANACO, MTN or Airtel, or make up a name that sounds official. Some pretend to be from a business you know, like a utility company such as Kafubu Water, a tech company, or even a charity organisation asking for donations. They use technology to change the phone number that appears on your caller ID. So the name and number you see might not be real.

Scammers say there's a "PROBLEM" or a "PRIZE"
They might say they are from Airtel, and that since you are an Airtel subscriber, there appears to be issues with validation with your Simcard and so, they may need to validate your Simcard systematically, by verifying your personal details *(NRC number, Pin and so forth).* Once you avail them your personal details, they may deregister your Simcard, reregister it and change your mobile money PIN and withdraw all the funds that might have been in your mobile money account without you knowing anything until it is too late for you to realise or counter act.
Or, they may say that you have won money, but you need to send specific details and be charged a small fee for you to claim your prize. Or that MTN is giving away prizes to their long staying subscribers but you need to pay a small fee for you to claim your rewards or so.

Scammers "PRESSURE" you to act immediately.
Scammers want you to act before you have time to think. If you are on the phone, they might tell you not to hang up so you cannot check out their story. They might

threaten to arrest you, sue you, take away your driver's or business license, or deport you. They might say your computer is about to be corrupted.

Scammers tell you to "PAY" in a specific way

They often insist that you pay by sending money through a money transfer company or by putting money on a gift card and then giving them the number on the back. Some will send you a check (that will later turn out to be fake), tell you to deposit it, and then send them money.

Mitigation Measures against Online Scams (What You Can Do to Avoid a Scam)

- ✓ Block unwanted calls and text messages. Take steps to block unwanted calls and to filter unwanted text messages.
- ✓ Do not give your personal or financial information in response to a request that you did not expect. Legitimate organizations will not call, email, or text to ask for your personal information, like your Social Security, bank account, or credit card numbers.
- ✓ If you get an email or text message from a company you do business with and you think it is real, it is still wiser not to click on any links. Instead, contact them using a website you know is trustworthy. Or look up their phone number. Do not call a number they gave you or the number from your caller ID.
- ✓ Resist the pressure to act immediately. Legitimate businesses will give you time to decide. Anyone who pressures you to pay or give them your personal information is a scammer.
- ✓ Know how scammers tell you to pay. Never pay someone who insists you pay with a gift card or by using a money transfer service. And never deposit a check and send money back to someone.
- ✓ Stop and talk to someone you trust. Before you do anything else, tell someone — a friend, a family member, a neighbour — what happened. Talking about it could help you realize it is a scam.
- ✓ Check the categories under which the social media page has been categorised by the creator of the page. For example, an electronics store social media page will be categorised as 'Electronics' and not politics.
- ✓ Official social media profiles can receive numerous tags and messages by the day, hour or even minute depending on their type. Check out how a profile engages with followers and be suspicious of profiles that post spam or only showcase deals that seem too good to be true.
- ✓ Always read all the fine print contained in a loan facility to see if there may be any hidden charges that may disadvantage you at a later stage.

Strategies which the Commission may Endeavor to Use to Detect Scams and to Raise Awareness to the Members of the Public

With the current COVID-19 Pandemic, more people are now spending most of their time online carrying various transactions and other activities. On average, 6 hours is spent online in a day. With this, the Commission needs to find ways to identify cases online and sensitize members of the public. Below are some of the strategies that the Department can explore;

1. Update the Commission's Website and Social Media Platforms

An update of the Commission's Website (under Consumer Protection Column) with subjective information on various categories of Scams and respective preventive measures, which Consumers NEED to learn, would be a milestone tool for raising awareness and sensitization for the Commission.

Implementation

1.1 The Consumer Department shall need to work in conjunction with the IT department to ensure that the much-needed information on Scams is drafted and uploaded on the Commission's main Website and Social Media Platforms. ***(CIs shall assign tasks and stipulate timeframe for the exercise)***

2. Production of Short Video Adverts Depicting Detection and Prevention of Scams

A production of short video adverts depicting detection and prevention of online scams and have them played on television during prime time is another effective way of raising awareness to the members of the public, given the current rate of online transactions by members of the public.

Implementation

2.1 The Consumer Department shall need to work in conjunction with the PR department to ensure that the much-needed information scripts on Scams is drafted and produced in various languages for play at television stations. ***(CIs shall assign tasks and stipulate timeframe for the exercise)***

3. Development of Brochures Specifically on Online Scams, How to Detect them and the Preventive Measures that Need to be Undertaken by Consumers against Online Scams

A Development of brochures specifically on online scams concerning how to detect them and the preventive measures that need to be undertaken by consumers against online scams is also another effective way sensitization especially to Consumers in the rural areas who may not have access to televisions or radios.

Implementation

3.1 The Consumer Department shall need to work in conjunction with the PR department and other relevant experts/consultants to ensure that the much-needed information on Scams is drafted and published in both the official language and various local languages for distribution across the country. ***(CIs shall assign tasks and stipulate timeframe for the exercise)***

4. Sensitize the Public on Online Scams via Departmental Media Programs

The Consumer Department Should incorporate online scams topics in the sensitizations via radio and television programs as a way of also raising awareness among members of the public.

Implementation

4.1 Officers (PIs and Is) in the Consumer Department shall need to work in conjunction with the PR department to ensure that during their respective radio and TV programs, they highlight and explain critical matters on online scams and how to prevent against falling victim to scammers in different local languages. ***(PIs and Is to implement this during their radio and tv programs)***

5. Internet Sweep

Social media platforms have proven to be useful as a source for certain case information. Perusal of particular pages of interest on the below platforms can provide information on contraventions of the Act, that may be prevailing in the market;

(a) *Facebook*
(b) *Twitter*
(c) *LinkedIn*
(d) *WhatsApp*
(e) *Pinterest*
(f) *Instagram*

Implementation

5.1 Officers in Consumer Department to actively share the Commission's Facebook/Twitter page and review comments to identify potential consumer issues. Each officer shall be required to implement this by searching for any matters that may be of interest to the Commission at least once a week from between 08:00 hours and 17:00 hours on the platforms identified. This could be done on a weekly basis, say every Fridays by two officers, one in each region; ***(CIs to come up with a draft timetable for officers).***

A Brief report shall be required from each officer within 24 hours of execution of the activity.

6. Desktop Search

The Commission's officers to review terms and conditions of various institutions including financial firms, that may be available on their websites such as

- ✓ Publications
- ✓ Websites
- ✓ Adverts
- ✓ Current Affairs
- ✓ Advertisements
- ✓ Any other information that may be of interest to the Commission pursuant to the CCPA.

Implementation

6.1 Each officer shall be required to implement this by searching for any matters that may be of interest to the Commission at least once a week from between 08:00 hours and 17:00 hours on the platforms identified. This could be done on a weekly basis, say every Fridays by two officers, one in each region; ***(CIs to come up with a draft timetable for officers).***

A Brief report shall be required from each officer within 24 hours of execution of the activity.

7. *Agency Collaboration (Local, Regional, and International)*

Local Collaborations

Use of Memorandum of Understandings (MoUs) with Sector Regulators such as ZICTA, *(Tip offs, joint working committees and other forms of information sharing)* and re-establishing contacts where it was lost or is inconsistent to help get abreast with proactive and current mitigating measures on possible online scams.

Implementation

7.1 Strengthening all existing MOUs and identifying relevant stakeholders with whom to implement collaborative efforts. This shall be done in liaison with the Research and Education Unit and any other departments that may have suggestions to move this collaboration forward. Reminder letters, virtual meetings and joint operations may be employed in this regard. Conduct a review of existing MoUs and signing of new ones to capture all relevant stakeholders key to combating the vice holistically.

8. Regional Collaborations

Use of MoUs with regional bodies like COMESA Competition Commission (Tip offs, joint working committees, capacity building initiatives and other forms of information sharing).

Implementation

8.1 The Consumer Department through the office of the CA may send various letters and/or emails to concerned regional bodies requesting to share best practices and mirror operations, among others.

9. International Consumer Protection Agencies

Mirror operations with regional and international Consumer Protection Agencies (CPAs) will provide us with information on new trends and best practices in enforcement of Consumer Protection.

Implementation

9.1 Webinars, teleconferences, publications, and monitoring of operations of international networks like ICPEN, AD, OECD and UNCTAD shall be conducted by the Department when and is scheduled.

10. *Confidential Informants & Surveillance Operations*

The Consumer Protection Department needs to access sources of sensitive economic information and methods of conducting secret surveillance operations. This could be achieved through the following.

(a) Peers – Friends and colleagues may be willing to divulge or volunteer information which may be of use to the Commission.

(b) Employees – Some staff members of sensitive institutions may become Confidential Informants of the Commission.

(c) Whistleblowers – Need to scout for citizens who may have sensitive information to come forward and give details of such.

(d) Security Wings – Various security wings deal with cases which they may not border on our Act and hence re-engagement of contact persons or establishing contacts where we may not have is very important.

(e) Screening – Market surveillance operations aimed at identifying recurrent and emerging consumer issues which may be of concern to the Commission.

6.1 **Implementation**

This shall require training by security wings in intelligence gathering, investigative techniques and conducting of secret surveillance operations. Security wings such as the DEC, FIC, ZP and other relevant security wings may be called upon to assist in this regard. Therefore, the Department of Consumer Protection may come up with programs aimed at quipping the officers with such skills.

Conclusion

The implementation of the above methods is aimed at enhancing productivity for the Commission, sharpening investigative and intelligence gathering skills, ensuring that there are reduced incidences of contraventions of the Act. An appropriate monitoring and evaluation method shall be employed at suitable intervals to measure the effectiveness of the various techniques cited in this paper and shall be governed by the strategic plan, work plans and assigned performance benchmarks. All the methods identified shall be implemented in a cost-effective manner and within the Ministry of Health guidelines of prevention of the Covid-19 pandemic and the 'new normal'.

Recommendations

The Department of Consumer Protection therefore recommends that:

(i) The Commission facilitate the actualization and achievement of the aforementioned strategies.

(ii) The Commission writes to the DEC and ZP and other relevant security wings for periodic departmental training in investigations, handling confidential informants and conducting surveillance operations among others;

(iii) The Commission sets up a joint working committee with the DEC and ZP whilst strengthening collaborative and information sharing initiatives with the FIC, BoZ, PIA, SEC, CUT, ZICTA and international CPAs;

(iv) The Commission must explore ways to effectively collaborate with the Smart Zambia institute to supplement the collaborative initiatives ongoing with ZICTA;

(v) The Commission collaborates with ZICTA to identify and prosecute local perpetrators of online scams in line with the Cyber Security and Cyber Crime Bill.

(vi) The Commission must strive to look at new sources of information such as the Auditor General's report and training of parliamentarians which may yield benefits as they may bring forth matters arising from their constituencies;

(vii) The Commission should employ appropriate periodic methods to monitor and evaluate the effectiveness of the methods to be employed herein.

(viii) The Commission and other stakeholders to send alert short message services (SMS) to mobile phone users on the various mobile scams.

(ix) The Commission and stakeholders to conduct continuous awareness campaigns through various platforms to combat the ever-changing types of scams.

(x) The Commission to engage ZICTA on developing strategies on how to identify perpetrators of online scams at local level in line with the Cyber Crime Bill.

(xi) The Commission to collaborate with the Bank of Zambia to sensitizing consumers on get rich quick Ponzi schemes.

The End

By Mr. Chipapa Matyola and Mr. Joseph Kaumba **June, 2021**

References

1. https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams
2. ANSI (American National Standards Institute) and BBB (Better Business Bureau) (2008) ANSI-BBB Identity Theft Prevention and Identity Management Standards Panel Final Report, 31 January 2008,
3. www.ansi.org/standards_activities/standards_boards_panels/idsp/report_webinar08.aspx? menuid=3. BWGCBMMF (2004), Report on Identity Theft, report to the Ministry of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States, October 2004,
4. www.ps-sp.gc.ca/prg/le/bs/report-en.asp. EC (European Commission) (2006), DG SANCO, Special Eurobarometer, Consumer Protection in the Internal Market, September 2006, Brussels, http://ec.europa.eu/public_opinion/archives/ebs/ebs252_en.pdf.
5. FTC (Federal Trade Commission) and DOJ (Department of Justice) (US) (2007a), Combating Identity Theft: A Strategic Plan, US President's Task Force on Identity Theft, 23 April 2007, www.idtheft.gov.
6. FTC (2007b), Report on Consumer Fraud and Identity Theft Complaint Data, www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf.
7. https://www.consumer.ftc.gov/articles/how-avoid-scam
8. Strategies for Case Initiation & Effective Institutional Collaboration in Covid-19 & Beyond; CCPC, DRBP, June, 2020