

Unclassified

English - Or. English

7 November 2023

**DIRECTORATE FOR FINANCIAL AND ENTERPRISE AFFAIRS
COMPETITION COMMITTEE**

Global Forum on Competition

Use of Economic Evidence in Cartel Cases – Contribution from Kenya

- Session III -

7-8 December 2023

This contribution is submitted by Kenya under Session III of the Global Forum on Competition to be held on 7-8 December 2023.

More documentation related to this discussion can be found at: oe.cd/egci.

Please contact Ms Lynn Robertson if you have questions about this document
[Lynn.Robertson@oecd.org]

JT03531128

Use of Economic Evidence in Cartel Cases

- Contribution from Kenya -

1. Introduction

1. Cartels are considered the most egregious infringement of competition law. The median cartel price overcharge shows that, for example, in the European Union and in some developing countries, it is estimated at 20% and only slightly lower (between 16.7% and 19%) in the US and Canada¹. Cartels restrict healthy economic growth, drive up prices, and reduce innovation and investment. Given these consequences, the discovery, investigation, and prosecution of cartel conduct is an enforcement priority of competition authorities, across the world.

2. Evidence gathering is a key ingredient to a cartel investigation. Competition authorities rely on evidence to prove the existence of a cartel, its scope, the involvement of undertakings, and the duration of the illegal conduct. Therefore, competition agencies may adopt digital tools to strengthen their fight against cartels, which may allow them to search through high volumes of data in a swift manner and with a high degree of accuracy.

3. In Kenya, the competition law is enforced by the Competition Authority of Kenya ('the Authority') which is mandated to promote and safeguard competition in the national economy and protect consumers from unfair and misleading market conduct.

4. Cartels are perpetrated through agreements by undertakings including trade associations. The hardcore agreements under the Act are classified as offenses, they include conducts such as price fixing, allocation of markets, output restrictions, and bid-rigging schemes². Hard-core cartels create market power, waste, and inefficiency in countries whose markets would otherwise be competitive³ and inflate the cost of living robbing its citizens of disposable income.

5. The Authority uses a combination of software and statistical methods to detect and remedy cartel conduct. There has been a continuous digitalization of private businesses and public services resulting in increased availability of data in digital form which has contributed to making it harder to detect anticompetitive practices. Digital tools therefore support the gathering of digital evidence in cartel enforcement. Digital forensics, in particular, is now being used by the Authority for the copying and analysis of evidence found during inspections and to deal with very large amounts of data in an efficient manner.

6. Additionally, the Authority uses both proactive and reactive methods to detect possible competition law infringements and subsequently launch investigations. In conducting its investigations, the Authority is guided by section 31 of the Act which provides for the process of investigation. It may upon receiving a complaint or on its own

¹ DAF/COMP/LACF(2020)2

²

<https://cak.go.ke/sites/default/files/Consolidated%20Guidelines%20on%20Restrictive%20Trade%20Practices%20.pdf>

³ <https://www.oecd.org/competition/cartels/21552797.pdf>

motion (*suo moto*), decide to conduct an investigation by issuing a Notice of Investigation to the accused party informing it that it is the subject of an investigation and the contents of the complaint or violation.

7. Evidence gathered can be classified as direct or circumstantial evidence. The Authority relies on both direct evidence, such as documents, written or oral statements that directly describe an infringement, and circumstantial evidence which can come in different forms, including communication evidence between undertakings (e.g. records of telephone conversations, minutes, emails, social media messages, notes) and economic evidence.

8. This contribution highlights the Authority's evidence-gathering process, and challenges encountered during the extraction of evidence, and proposes a way forward.

2. Evidence Gathering tools and Processes applied by the Competition Authority of Kenya

9. Evidence gathering by the Competition Authority of Kenya is guided by sections 31, 32, 33 and 89 of the Act. Section 31 provides powers to the Authority to investigate allegations of an anticompetitive nature on its own motion or upon receipt of a complaint. It gives the Authority extensive powers to obtain information through the issuance of notices of investigation and requests for information. Section 32 empowers the Authority to enter and search the premises of suspected cartel participants and get information therein. Section 33 empowers the Authority to receive disclosures from third parties through the recording of statements under oath. In addition, Section 89 empowers the Authority to issue leniency policy guidelines to enhance and facilitate investigations and enforcement actions by encouraging undertakings that have been engaging in wrongdoing to provide direct evidence and proactively cooperate in bringing successful enforcement action in return for full or partial immunity.

10. In order to enhance its evidence-gathering capability, the Authority rolled out the leniency program guidelines in 2017. It also developed an informant reward scheme policy in 2021 which also increased its efficiency in the detection and enforcement of restrictive trade practices through the usage of the informant reward scheme.

11. Oftentimes, cartel participants hide their conduct and unless detected, the conduct can continue for an inordinate period. In the recent past, the Authority has received complaints through intelligence on alleged cartel conducts in the market. In order to increase its ability to detect the cartels that may be covertly existing in the market, the Authority has adopted the use of screenings, market inquiries, monitoring the markets, and inter-agency collaboration as useful tools to detect cartels and gather initial evidence on the existence of cartels. These methods provide a basic set of evidence to investigate the affected sectors.

12. When the Authority undertakes a market screening as a source of gathering initial evidence, it undertakes a complete review of a sector by undertaking both structural and behavioral reviews of the market. Structural screening includes analysis of structural and product characteristics of a specific market or industry that make successful collusive strategies more likely. It is based on what economic theory and empirical research tell us about the relationship between market characteristics and the likelihood of collusion occurring in markets. The structural market screening involves a cross-industry or cross-market search for those characteristics that are known to facilitate cartelization, or that have been exhibited in cartelized industries in the past.

13. Some of the factors that the Authority looks out for include structural (small number of competitors, high entry barriers, frequent interactions, and market transparency); supply-

related (mature stage of an industry, the low pace of innovation, symmetry and commonality of costs and product homogeneity) and demand related (stable demand conditions, low demand elasticity, buying power, and the absence of club and network effects.) However, structural screens require readily available data which may not always be present in most industries. Structural screens only point at markets that exhibit a propensity for collusion rather than providing agencies with preliminary evidence of collusion.

14. The behavioral screening of the market, on the other hand, involves outcome-based analysis founded on a variety of variables such as prices, quantities, market shares, and bidding decisions. Some of the behaviors the Authority looks at include increased prices and more uniform prices, a series of steady price increases preceded by steep declines if there are prices rise but imports decline, if firms' prices are strongly positively correlated if there is a reduced variance of price, periodic switching between high and low-price levels (structural shifts) and discontinuing of discounts that were previously common.

15. The Authority uses these proactive detection tools for market screenings and market inquiries as may be required for different market circumstances. If the findings from the screenings are positive as to the likely existence of a cartel, the Authority invokes section 32 of the Act. This section 32 empowers the Authority to gather evidence through the entry and search⁴ to obtain evidence on conduct prohibited under sections 21, 22, and 24 of the Act (*price-fixing agreements, output restriction, and market division agreements, among others*).

16. The Authority can search the electronic devices of the firms' available staff, and with the aid of digital tools and physical verifications to the premises may search any data contained in or available to that computer system, reproduce any record from that data, seize any output from that computer for examination and copies, attach and, if necessary, subject to the issuance of a receipt to that effect, remove from the premises for examination and safekeeping anything that has a bearing on the investigation.

17. As per section 32(4) of the Act, the Authority is permitted to seek the assistance of police officers and other law enforcement agencies in the execution of its mandate. The Authority has also in recent cases utilized the services of the Ethics and Anti-corruption Commission to mine and analyze evidence using the Commission's tools. Additionally, section 9(m) of the Act provides that the Authority may liaise with regulatory bodies and other public bodies in all matters relating to competition and consumer welfare. Additionally, pursuant to section 13(2) of the Competition Act which provides that the Authority may engage consultants and experts to assist it in performing its functions and exercising its powers. The Authority also contracts forensic laboratory experts who assist in the extraction of information from mobile phones and laptops when a need arises.

18. We work to ensure that the evidence is obtained and preserved without risk of tampering by employees of the accused firm(s). In its previous engagements of investigating cartel conducts in the **cement, paints, and steel sectors**, the Authority used digital tools and techniques to gather evidence. The Authority has also trained its staff on evidence gathering using various equipment and software and where it does not possess the technical know-how or equipment, it has been seeking the help of consultants.

19. Following the extraction of information, the Authority invites the owners of the devices, who appear before it, to verify the extracted information for confirmation.

⁴ <https://cak.go.ke/sites/default/files/Competition-Act-No-1-%20of%202010-Amended-as-at-2019.pdf>

Box 1. Onsite evidence gathering

In 2021, the Authority while conducting an investigation in the steel sector, raided 13 steel manufacturing companies. The investigation team and forensic experts (engaged by the Authority pursuant to section 32(2) of the Act) were able to extract the relevant files from computers, laptops, iPads, tablets, and phones by creating forensic images that were stored in (USB sticks or hard disks).

The Authority also extracted information from annual reports, draft audited financial statements, various pricelists and internal reports, and emails on input costing and pricing. The Authority retained those devices which were not accessible due to the unavailability of passwords and which the extracting equipment was not able to ethically hack the passwords. All the extracted data was then indexed and later reviewed by the investigative team of the Authority.

After the images were created, the Authority returned the devices to the companies' staff who came to the Authority and confirmed the items and documents picked and signed an inventory sheet for the return of items. In the process of mining the said data, the Authority came across communications that contained infringing information used to perpetrate a violation of the provisions of the Competition Act.

20. After the search and seizure exercise, the Authority forwards desktops and hard drives to the forensic consultants for extraction of the digital information, after which they generate a report that includes the certificate of electronic record. In doing so, it ensures that the electronic evidence obtained from the parties under investigation is reasonable and procedurally obtained in a fair manner as envisaged under the 2010 Constitution of Kenya, Competition Act, and Fair Administrative Action Act, 2015.

21. The Authority also obtains a certificate of electronic record by the Evidence Act for purposes of rendering its evidence admissible before a court of law just in case the matter goes for full prosecution.

2.1. Analysis of Digital Evidence

22. Once the Authority collects the evidence, much work goes into analyzing it and generating reports on digital evidence in a format that is legally admissible in a court by using forensic examiners or computer forensics experts who apply different types of digital forensic techniques and tools. The analysis uses a keyword searching method with keywords derived from desk research, informants, leniency applicants, or explanations sought during the on-the-spot inspection in its digital evidence analysis.

2.2. Notice of Investigation and Interviews

23. After assessing and determining culpability, the Authority issues further Notices of Investigations and Summons for Appearance to the parties of interest pursuant to Section 31 of the Competition Act. The accused parties are invited to appear for interviews which enables the Authority to collect more information. Upon conducting the interviews, if the Authority is convinced of the existence of cartel conduct, it issues a Notice of Proposed Decision pursuant to Section 34 of the Act.

3. Challenges of Evidence Gathering

24. As explained earlier, the Authority relies on both direct or circumstantial evidence which may either be physical or digital evidence in its investigation process. The bulk of the Authority's evidence is normally acquired through searches as stipulated in section 32 of the Act.

25. After the Covid-19 crisis hit the world, companies accelerated towards moving their paper-based operations online. This has presented a multifaceted challenge for the Authority in detecting cartels as well as gathering the necessary evidence during investigations. Below are some of the challenges the Authority faces in gathering evidence:

3.1. Legal Challenges

3.1.1. Acquiring of Search Warrants and execution

26. Getting the search warrants may prove to be a challenge unless the magistrate understands the reasons why the Authority is resorting to dawn raid as opposed to other available means in gathering or obtaining evidence.

27. Additionally, when electronic data is seized during dawn raids, the Authority targets computers, servers, mobile phones, laptops, and other electronic storage devices. Care has to be taken to ensure that the warrant authorizes the search and seizure and also authorizes the seizure of data on laptops or other devices not on the premises, or access may not be granted thereto.

Box 2. The High Court Rules on Authority's First Search & Seizure Operation

The Authority investigated the fertilizer sector in 2016 and invoked its powers under Section 32 which allows carrying out of dawn raids and it therefore conducted searches on two firms in the sector. A constitutional petition was subsequently lodged by one of the parties that was raided, on the constitutionality of the Authority's search process.

The party through an interlocutory application in the petition sought an injunction to bar the Authority from proceeding with further investigations on the grounds that the search and entry were unlawful. It was alleged that the party was not notified of the search which was a breach of its rights under Article 47 of the Constitution, 2010. Moreover, it was argued that the search warrants were obtained through concealment, gross misrepresentation, abuse of office, and the fact that there was no reasonable suspicion of a criminal offense.

The Authority argued that it carried out a legitimate search as provided under Section 32 and had lawfully obtained the requisite search warrants. The Court in its ruling found that the Authority acted within its statutory mandate under Section 32 of the Competition Act which provides that the Authority may in its investigation search the premises of parties. The Court further agreed with the Authority's position and found that the search warrants were obtained lawfully.

The Court ruled that an investigator is not legally obliged to give notice prior to a search depending on the circumstances. It was upheld that the Authority and its officers had acted within the law and in good faith. This is a big step in creating legal precedence on the mandate of the Authority to investigate anti-competitive practices in the public interest. It is important to note that the party withdrew its main petition and opted to settle the matter out of Court.

3.1.2. Protection of confidential information and legally privileged documents

28. Dealing with confidential and privileged information poses a challenge in gathering evidence. Sometimes an undertaking may claim that the seized information obtained during the raid is privileged information. Therefore, in as much as there is a need to ensure adequate measures are put in place to protect the company's legally privileged and highly confidential documents, the Authority needs to sieve through the evidence to ensure that the relevant information related to the investigations is not concealed under the confidentiality cover.

3.1.3. Acquisition, Handling and Managing Digital Evidence Challenges

29. Handling and managing evidence is one of the key challenges the Authority faces in its enforcement activities. In particular, digital evidence is increasingly becoming a core part of all investigations, ever-increasing in size, and creating multiple problems with digital evidence when it comes to handling and managing them.

30. The increasing amount of digital evidence obtained during raids creates more avenues for law enforcement officers to solve cases. Still, it can be inadmissible in court if it is not handled properly, or its integrity is not being preserved at any level. In this regard, below is a list of challenges the Authority faces while handling digital evidence.

3.2. Technical Challenges

3.2.1. Forensic Tools

31. During the course of searches and seizures, the Authority highly relies on forensic tools to acquire evidence. Digital forensic tools and equipment provide the Authority with automated capabilities, based on previous professional knowledge and criteria, which can be used to verify and validate the state of evidence. However, these tools are expensive and are ever-evolving hence with scarce resources the Authority struggles to keep pace with the acquisition of new tools in the advancement of the technology.

3.2.2. Collection of the evidence

32. Chain of custody is another challenge that the Authority seeks to always address during the evidence-gathering process. Before evidence is collected during a raid it is important to document steps of the process. Documentation is needed throughout the entire investigative process (before, during, and after the evidence has been acquired). The Authority maintains an inventory that includes detailed information about the digital devices collected, including the operational state of the device - on, off, standby mode - and its physical characteristics, such as make, model, serial number, connections, and any markings or other damage. The digitally collected evidence has to be validated with a digital certificate to confirm the authenticity of the process.

3.2.3. Risk of Data Breach, Tampering, and Cyber Attacks

33. Collecting digital evidence is easy in most cases. The tricky part is securing and protecting it from data breaches, cyber-attacks, and tampering. It is very challenging to prevent these attacks and detect tampering as it is done discreetly to make it seem like the evidence is still intact.

3.2.4. Data Encryption

34. Encryption can make it difficult to access the data on a device or network, making it harder for forensic investigators to collect evidence. This can require specialized decryption tools and techniques. In recent searches, encryptions have been noted in the latest models of i-phones and it therefore means the Authority has to procure mobile phone forensic imagers of higher capability.

3.2.5. Analysis of a high volume of electronic evidence

35. The use of forensic tools in data mining during raids has enhanced the Authority's capability of extracting huge amounts of raw digital evidence. However, the challenge of analyzing these volumes of data requires high processing times hence leading to high backlogs. Serious implications relating to increasing backlogs include; the long time taken by the Authority to conclude an investigation and make a final decision; a case example being the steel sector investigations which were carried out for three years. In such circumstances, section 13(2) of the Act permits the Authority to engage consultants and experts to assist it in performing its functions and exercising its powers. During searches, the consultants using different forensic tools (FTK, Detego, Forensic Imager (TX1), and Mobile phones & devices extraction tools) which helped the Authority in extracting information from desktops and hard drives.

36. These forensic services are expensive and unsustainable hence the Authority in a bid to expand its enforcement frontiers, is planning to build capacity for the utilization of digital forensics by setting up a forensic laboratory (lab) that will assist in forensic investigations.

4. Conclusion and Way forward

This paper has explained the evidence-gathering process by the Authority as well as the challenges it encountered in the process of collecting evidence.

37. Some of the proposed solutions for the above challenges include the how and why to obtain search warrants. It is common for the search warrants to authorize the Authority's staff to undertake an electronic search of a firm's records (which can include personal devices if they are on the premises and the Authority has reason to believe they contain information relevant to the investigation). A challenge arises in explaining to the magistrate the reason why the Authority is resorting to dawn raid as opposed to other available means in gathering or obtaining evidence. The Authority therefore needs to be clear and sancit in its requesting applications to the courts as far as the scope of the raid is concerned.

38. Secondly, documents that are protected by legal professional privilege, such as legal advice provided to an undertaking by its legal advisers, are not required to be disclosed to most of the competition agencies. However, the challenge arises when an undertaking declares the seized information obtained during a raid as privileged information. Therefore, in as much as there is a need to ensure adequate measures are put in place to protect the company's legally privileged and highly confidential documents, the Authority has endeavored to have a search and seizure guideline to address the process of identifying and handling legally privileged information.

39. Thirdly, the forensics tools that most of the competition agencies rely on are expensive and are evolving hence with scarce resources the competition agencies struggle to keep pace with the changes in the advancement of technology. There is a need to explore the most efficient and cost-effective tools to be used in gathering digital evidence.

40. Additionally, there is a need to upskill the capacity of forensic investigators to bolster investigation efforts for the competition agencies by allowing for the recovery of hidden and deleted information, recovery of evidence from damaged equipment, harvesting data, and eliminating or filtering evidence. This will help improve the quality of decisions made by the competition agencies by assisting with the retention of evidence authenticity and generating digital evidence that can be relied on even in criminal proceedings pursued through the courts.