OECD publishing

IMPLEMENTATION TOOLKIT ON LEGISLATIVE ACTIONS FOR CONSUMER PROTECTION ENFORCEMENT CO-OPERATION

OECD DIGITAL ECONOMY PAPERS
June 2021 **No. 310**

OECD
BETTER POLICIES FOR BETTER LIVES

Foreword

This Implementation Toolkit on Legislative Actions for Consumer Protection Enforcement Co-operation ("the Toolkit") builds on and aims to support the implementation of the principles on cross-border enforcement co-operation contained in the 2003 OECD Recommendation Concerning Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices across Borders [OECD/LEGAL/0317] and the 2016 OECD Recommendation on Consumer Protection in E-commerce [OECD/LEGAL/0422]. It also builds on the Committee on Consumer Policy's (CCP) 2018 study on cross-border enforcement co-operation ("the 2018 OECD study") (OECD, 2018[1]) and the CCP's roundtable held on this topic in October 2019 (OECD, 2020[2]).

The Toolkit is directed at helping countries reduce the "legal authority" barrier to cross-border enforcement co-operation identified in the 2018 OECD study. It is neither an OECD legal instrument nor a model law. Instead, it is a practical resource for consumer protection enforcement agencies that do not currently have the domestic legal authority needed for such enforcement co-operation to make the case for obtaining relevant legislative tools, and provides guidance to ensure that related legislative reforms are fit for purpose. It does not preclude other methods of implementation through mechanisms such as soft law and bilateral or multilateral arrangements.

The Toolkit sets forth ten guiding principles on legal and operational issues relating to: i) investigatory powers, ii) enforcement outcomes, and iii) co-operation practices. To help jurisdictions develop specific enabling legislation, statutes, and rules, the Annex provides a rationale for each guiding principle as well as examples of cases of cross-border enforcement co-operation and related statutory text from jurisdictions, including from the product safety, competition, privacy and financial securities policy areas.

This paper was prepared by the United Kingdom and the United States, with drafting assistance from the European Commission and the OECD Secretariat. It was approved and declassified by the CCP on 12 April 2021 and prepared for publication by the OECD Secretariat.

Note to Delegations:

This document is also available on O.N.E under the reference code:

DSTI/CP(2020)5/FINAL

This document, as well as any data and any map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

© OECD (2021)

The use of this work, whether digital or print, is governed by the Terms and Conditions to be found at http://www.oecd.org/termsandconditions.

Table of contents

FIGURES

1 Introduction

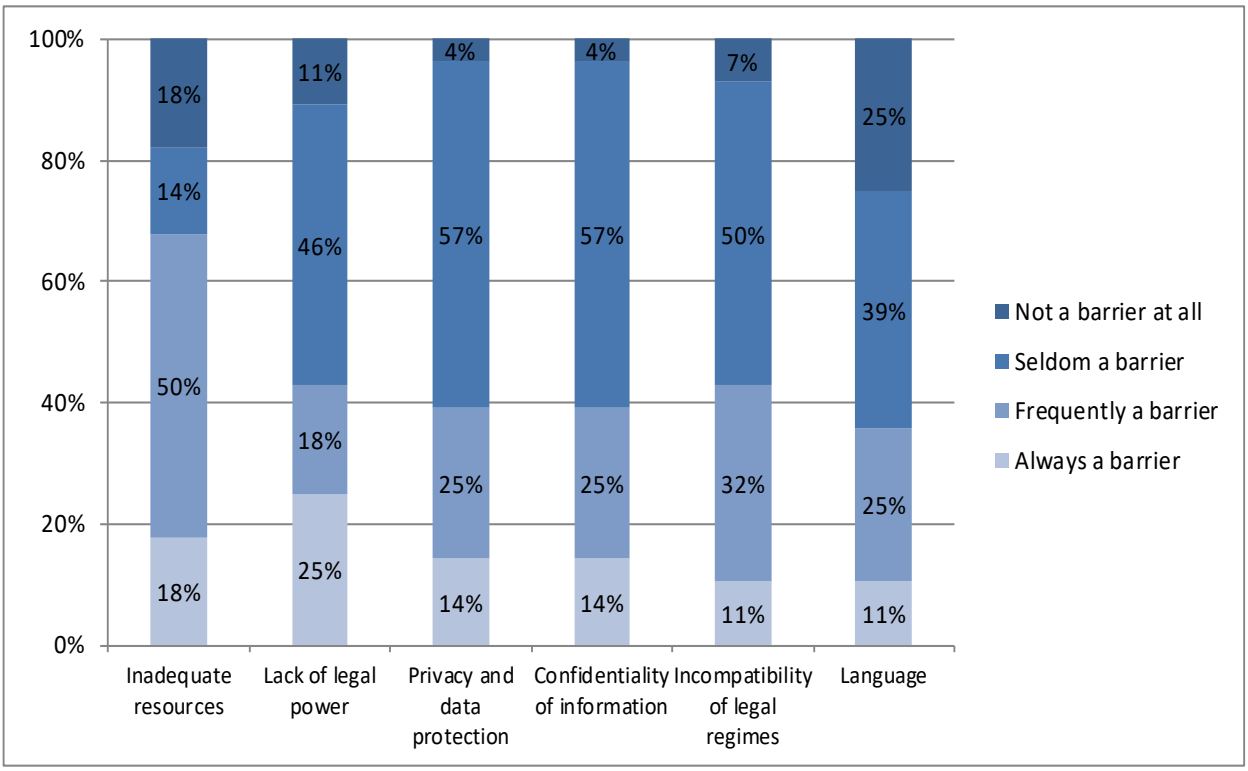
Ongoing obstacles to cross-border enforcement co-operation

The digital transformation has changed how businesses operate and how consumers purchase goods and services at domestic and global levels. Online businesses today enable consumer transactions in multiple jurisdictions. While providing consumers with numerous benefits, such as increased product choice at competitive prices, this inevitably causes periodic consumer problems, and the cumulative harm to consumers that results is substantial in a number of countries. Between January 2015 and June 2020, for example, the Consumer Sentinel complaint database of the United States (US) collected more than 657 629 complaints from US and non-US consumers against foreign businesses from all over the world, including Canada, India, Jamaica, Mexico, Nigeria, the People's Republic of China, the United States, and the United Kingdom.[1]

When problems with a cross-border consumer transaction arise, evidence may not physically be in the place where an investigation is being carried out, and may instead be located overseas. Moreover, some businesses operating across borders can today exploit new technologies, such as artificial intelligence, telephone number spoofing and digital currencies, to scam consumers remotely and steal their money and data. These conditions increase the need for more effective and coordinated approaches to cross-border enforcement co-operation for consumer protection.

Although countries have made significant efforts in developing domestic, regional[2] and international frameworks for consumer protection and enforcement co-operation across borders since the adoption in 2003 by the OECD Council of the Recommendation concerning Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices across Borders ("2003 Cross-Border Fraud Recommendation") [OECD/LEGAL/0317], many have not yet fully implemented all provisions. In 2018, the CCP reviewed the status of enforcement co-operation among OECD countries and some partner economies as part of a periodic review of the 2003 Cross-Border Fraud Recommendation. The Committee found that while many countries had engaged in some type of cross-border co-operation, a number of challenges to effective cross-border enforcement co-operation remain (OECD, 2018[1]). These include in particular a lack of adequate resources, insufficient legal authority, privacy and data protection limitations, confidentiality rules, and language issues. Approximately 90% of surveyed countries identified insufficient legal authority as one of the main barriers to cross-border enforcement co-operation in at least some circumstances, with 25% reporting that it was "always a barrier," and 18% reporting that it was "frequently a barrier." Similarly, 43% of countries reported incompatibility of legal frameworks as a barrier (see Figure 1).

Figure 1. Barriers to international co-operation in consumer protection



Source: OECD (2018[1]), based on 28 country responses

The report also noted that while some OECD countries had adopted legislation to facilitate cross-border enforcement co-operation, a number of the countries surveyed had not fully taken such steps. Further, it identified a lack of information about how co-operation pursuant to such enabling legislation actually occurs. It concluded that while the 2003 Cross-Border Fraud Recommendation and the 2016 OECD Recommendation on Consumer Protection in E-commerce ("2016 E-commerce Recommendation") [OECD/LEGAL/0422] have played an important role in establishing the principles to facilitate co-operation, "more efforts are needed to increase cross-border co-operation, including on notification and enforcement activities, such as information sharing and investigative assistance." A related report similarly concluded that the text of the 2003 Cross-Border Fraud Recommendation is "still fit for the purpose" but that better implementation of the core principles would help address problems that consumers face in cross-border markets (OECD, 2018[2]).

To further promote international co-operation for consumer protection, consistent with discussion in this area during the OECD's 2019 Ministerial Council Meeting (MCM) held in May 2019, the CCP organised a roundtable in October 2019 to share information about successful legal schemes implemented in jurisdictions to enhance cross-border enforcement co-operation (OECD, 2020[2]). The Committee highlighted the importance of adopting and enforcing domestic laws enabling consumer protection enforcement agencies to enhance cross-border co-operation, and the need to increase agencies' ability to co-operate across borders, in particular in the following three areas: information sharing, including of confidential information; investigative assistance; and securing outcomes. Following the discussion, the CCP agreed to develop a legislative guide on cross-border enforcement co-operation, in consultation with the International Consumer Protection and Enforcement Network (ICPEN).

Purpose of the Toolkit

This Implementation Toolkit on Legislative Actions for Consumer Protection Enforcement Co-operation ("the Toolkit") provides examples of how legislative action can support the implementation of policy principles on cross-border enforcement co-operation set forth in the 2003 Cross-Border Fraud Recommendation and the provisions on cross-border enforcement co-operation in the 2016 E-commerce Recommendation. It is also in line with the implementation of consistent consumer protection standards from other fora, in particular the 2015 United Nations Guidelines for Consumer Protection (United Nations, 2015[4]).

This Toolkit is neither an OECD legal instrument nor a model law. Instead, it is a practical resource for consumer protection enforcement agencies that do not currently have the domestic legal authority needed for such enforcement co-operation to make the case for obtaining relevant legislative tools, and provides guidance to ensure that related legislative reforms are fit for that purpose. Where appropriate, the Toolkit also points to non-legislative tools that consumer authorities have used to fill any legal gaps, including soft law tools and informal initiatives. The Toolkit does not, however, focus on the development of bilateral and multilateral agreements, which are needed in certain jurisdictions to enable cross-border co-operation between or among consumer protection enforcement authorities.

Indeed, there are many approaches to improving cross-border enforcement co-operation, as recognised in the Preface to the 2003 Cross-Border Fraud Recommendation: "countries have diverse consumer protection systems, involving different laws, enforcement procedures and roles for judicial authorities, and rely to varying extents on civil, criminal and administrative law." This diversity is reflected in the way jurisdictions have approached cross-border enforcement co-operation. Some have proceeded via binding international agreements, such as high-level government-to-government agreements (e.g. free trade agreements), while others have used non-binding memoranda of understanding and other agency-to-agency agreements.[3] In addition, others have relied on informal exchanges through peer-to-peer agency networks such as the ICPEN and staff exchanges. Most employ hybrid approaches, including elements of formal and informal co-operation. The European Union (EU) uses a multipronged approach through its Consumer Protection Co-operation (CPC) Regulation, which provides EU member states with a core set of enforcement powers, provides a mechanism for intra-European enforcement co-operation, and gives the European Commission a coordinating role for consumer protection law infringements, in particular when such infringements are widespread throughout the EU. Externally, the EU seeks binding international agreements to engage in cross-border enforcement co-operation with non-EU jurisdictions, while, internally, it relies on its EU member states' domestic procedural laws to carry out enforcement. In short, the Toolkit recognises that countries have conferred powers on their consumer protection enforcement authorities and can limit them through legislative actions or policy decisions in accordance with their legal framework.

Moreover, the Toolkit recognises that countries engage in cross-border co-operation through binding international, regional or bilateral agreements, such as the EU's CPC Regulation. Further, the Toolkit also recognises that countries can rely predominantly or entirely on international criminal enforcement co-operation mechanisms (e.g. mutual legal assistance agreements, extradition treaties) rather than cross-border civil or administrative co-operation tools when fraudulent commercial practices are classified as criminal offences and trigger criminal penalties in accordance with their legal framework. Accordingly, the Toolkit provides examples of legislative actions but does not recommend that countries rely on any one approach alone, given differences in systems of law, substantive consumer laws, and language. Instead, it presents a range of legislative options to assist countries that lack the legal capacity to engage in cross border co-operation due to gaps in domestic law or the unavailability of or constraints in using international criminal law mechanisms for fraudulent and deceptive commercial practices as explained in the Preface to the 2003 Cross-Border Fraud Recommendation.

Through the guiding principles, the Toolkit first explains why the issues covered are important. It then provides examples of statutory language addressing such key issues, as well as actual investigations and cases in jurisdictions. The Toolkit also provides guidance on legal and operational issues, along with actual enforcement and statutory examples, to help jurisdictions translate those high-level principles into specific enabling legislation, statutes, and rules that are consistent with the jurisdiction's legal framework. It recognises that the use of the Toolkit by interested countries is subject to constitutional and legal requirements or limitations of each jurisdiction, including laws on data protection and privacy, confidentiality, and principles of due process, international law, and mutual legal assistance.

OECD and other fora's principles on cross-border enforcement co-operation

The 2003 Cross-Border Fraud Recommendation establishes a common framework to combat cross-border fraud occurring online and offline through closer, faster, and more efficient co-operation between consumer protection enforcement agencies. The Recommendation sets out the key powers that consumer protection enforcement agencies need to have to effectively co-operate with their foreign counterparts, based on:

- Establishing a domestic system for combating cross-border fraudulent and deceptive commercial practices against consumers.
- Enhancing notification, information sharing and investigative assistance.
- Improving the ability to protect foreign consumers from domestic businesses engaged in fraudulent and deceptive commercial practices.
- Improving the ability to protect domestic consumers from foreign businesses engaged in fraudulent and deceptive commercial practices.
- Considering how to ensure effective redress for victimised consumers.
- Co-operating with relevant private sector entities.

The Recommendation also calls for Adherents to identify obstacles to effective cross-border co-operation and consider adopting or amending national legislation to overcome these barriers (Part II, E).

Following from the 2003 Cross-Border Fraud Recommendation, related OECD legal instruments were adopted to address enforcement co-operation, including the 2006 Recommendation of the Council on Cross-Border Co-operation in the Enforcement of Laws against Spam [OECD/LEGAL/0344], the 2007 Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy [OECD/LEGAL/0352], and the 2007 Recommendation on Dispute Resolution and Redress [OECD/LEGAL/0356], which contains recommendations for enhancing the effectiveness of consumer remedies in cross-border disputes.

Other organisations have adopted consistent high-level principles. The General Assembly of the United Nations (UN), for example, adopted in 2015 revised United Nations Guidelines for Consumer Protection ("UNGCP") (United Nations, 2015[4]) that encourage UN member states to "consider relevant international guidelines and standards on protecting consumers from fraudulent and deceptive cross-border commercial practices, in considering the legal authority to provide to their consumer protection enforcement agencies, and, where appropriate, adapt those guidelines and standards to their circumstances" (Paragraph 90). The UNGCP specifically refer to the 2003 Cross-Border Fraud Recommendation in advising member states "to study the Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices across Borders of the Organization for Economic Cooperation and Development" (Paragraph 90). The UNGCP also cite the 2016 E-commerce Recommendation to address issues in the context of e-commerce (Paragraph 65).[4]

The revised UNGCP added a section on international co-operation that draws on the 2003 Cross-Border Fraud Recommendation, and states that "Member States should provide their consumer protection

enforcement agencies with the authority to investigate, pursue, obtain and, where appropriate, share relevant information and evidence, particularly on matters relating to cross-border fraudulent and deceptive commercial practices affecting consumers. That authority should extend to co-operation with foreign consumer protection enforcement agencies and other appropriate foreign counterparts" (Paragraph 88).

The 2016 E-commerce Recommendation similarly recognises the need to "equip consumer protection enforcement authorities with the ability to effectively protect consumers in e-commerce and to exchange information and co-operate in cross-border matters" (Preamble). It contains expanded principles on cross-border co-operation, adopting many of the principles of the 2003 Cross-Border Fraud Recommendation for consumer protection in e-commerce more generally. In Part Two (Implementation Principles), it highlights that Adherents should:

> "iii) Establish and maintain consumer protection enforcement authorities that have the authority - and powers to investigate and take action - to protect consumers against fraudulent, misleading or unfair commercial practices and the resources and technical expertise to exercise their powers effectively;
>
> iv) Work towards enabling their consumer protection enforcement authorities to take action against domestic businesses engaged in fraudulent and deceptive commercial practices against foreign consumers, and to take action against foreign businesses engaged in fraudulent and deceptive commercial practices against domestic consumers."

Scope and structure of the Toolkit

To support the implementation of the above-mentioned OECD Recommendations, the Toolkit provides 10 guiding principles, which are grouped into the following three distinct areas:

- investigatory powers
- enforcement outcomes
- co-operation practices.

The Annex provides a rationale for each guiding principle, to elaborate on operational and legal issues, and to illustrate how these are especially relevant in practice. It sets forth examples of cases and legislation implementing these guiding principles from a broad range of OECD countries and partner economies, including from the product safety, competition, privacy and securities policy areas.

2 Guiding principles on cross-border enforcement co-operation for consumer protection

Overview

The Toolkit comprises ten guiding principles that are intended to support the implementation of both the 2003 Cross-Border Fraud Recommendation and the 2016 E-commerce Recommendation through domestic enabling legislation.

Specifically, the 2003 Cross-Border Fraud Recommendation provides for:

a. Establishing a domestic system for combating cross-border fraudulent and deceptive commercial practices against consumers.
b. Enhancing notification, information sharing, and investigative assistance.
c. Improving the ability to protect foreign consumers from domestic businesses engaged in fraudulent and deceptive commercial practices.
d. Improving the ability to protect domestic consumers from foreign businesses engaged in fraudulent and deceptive commercial practices.
e. Considering how to ensure effective redress for victimised consumers.
f. Co-operating with relevant private sector entities.

In particular, this Toolkit seeks to support the implementation of elements a, b, c and d, which focus on the detail of cross-border public enforcement.

In addition, this Toolkit aims to facilitate the implementation of Parts Two and Three of the 2016 E-commerce Recommendation that set forth policy principles on implementation and global co-operation to address issues in consumer transactions in e-commerce.

It should be noted that, in relation to some of the guiding principles, domestic enabling legislation would need to include appropriate procedural and substantive safeguards to the exercise of the recommended powers by consumer protection enforcement agencies in cross-border matters based on data protection and privacy, confidentiality, and principles of due process, international law, and mutual legal assistance. However, such safeguards ought not to prevent consumer protection enforcement agencies from the lawful exercise of their powers in appropriate cases or prohibit businesses or persons from co-operating voluntarily with a foreign consumer protection agency. Nor should such safeguards operate in a discriminatory fashion. In addition, domestic enabling legislation should provide for avenues for businesses and persons to challenge inappropriate use.

Area I: Investigatory powers

Guiding principle 1. Domestic investigatory powers

Principles for Cross-border Enforcement Co-operation for Consumer Protection from OECD Recommendations

The 2003 Cross-border Fraud Recommendation states that Adherents should provide for "Effective mechanisms to adequately investigate, preserve, obtain and share relevant information and evidence relating to occurrences of fraudulent and deceptive commercial practices" (Part II, A, 2).

The 2016 E-commerce Recommendation provides that Adherents should "Establish and maintain consumer protection enforcement authorities that have the authority and powers to investigate and take action to protect consumers against fraudulent, misleading or unfair commercial practices and the resources and technical expertise to exercise their powers effectively" (Part Two, Para 53 (iii)).

[See also UN Guidelines for Consumer Protection, Paragraphs V.A. 15, V.I.; 79 (a), 88.]

To implement the above recommendations, countries should provide their consumer protection enforcement agencies with the powers to:

a. Require the production of relevant information, including documentary, physical, or testimonial information from investigative targets and third parties, subject to relevant privileges, such as a privilege against self-incrimination in criminal matters.
b. Ascertain the identity of legal and natural persons engaged in commercial practices.
c. Seek to preserve evidence, particularly that of a transient nature, until it can be examined.
d. Compel production of relevant information administratively or judicially when necessary.
e. Carry out undercover investigations, in particular to gather evidence while acting in the role of a consumer.
f. Observe, including covertly when necessary, the conduct of business such as sales processes.
g. Inspect or search any premises or vehicle used for business related purposes when appropriate and lawful.
h. Access, seize and copy potential evidence, including digital evidence, irrespective of the storage medium or the place where the evidence is stored.
i. Require assistance and explanations from persons on the premises being inspected or searched.
j. Pursue sanctions for obstruction or failure to comply with evidence requests and orders.

Guiding principle 2. Application of investigatory powers to assist foreign consumer protection enforcement agencies

Principles for Cross-border Enforcement Co-operation for Consumer Protection from OECD Recommendations

The 2003 Cross-border Fraud Recommendation states that Adherents should improve "their ability to co-operate in combating cross-border fraudulent and deceptive commercial practices recognising that co-operation on particular investigations or cases under these Guidelines remains within the discretion of the consumer protection enforcement agency being asked to co-operate." It further states that the agency may "decline to co-operate on particular investigations or proceedings, or limit or condition such co-operation, on the ground that it considers compliance with a request for co-operation to be inconsistent with its laws, interests or priorities, or resource constraints, or based on the absence of a mutual interest in the investigation or proceeding in question" (Part III, A). It further provides that Adherents should "work toward authorising their consumer protection enforcement agencies, either directly or through appropriate mechanisms authorised by their judicial or administrative authorities, to obtain information, including documents and statements, and otherwise provide investigative assistance for foreign consumer protection enforcement agency investigations and actions, subject to appropriate safeguards" (Part IV, D).

The 2016 E-commerce Recommendation provides that Adherents should "Improve the ability of consumer protection enforcement authorities and other relevant authorities, as appropriate, to co-operate and co-ordinate their investigations and enforcement activities, through notification, information sharing, investigative assistance and joint actions." In particular, it provides that Adherents should "Simplify assistance and co-operation, avoid duplication of efforts, and make every effort to resolve disagreements as to co-operation that may arise, recognising that co-operation on particular cases or investigations remains within the discretion of the consumer protection enforcement authority being asked to co-operate" (Part Three, Para 54 (ii)).

[See also UN Guidelines for Consumer Protection, Paragraph VI.83, 88, 90.]

To implement the above recommendations, consumer protection enforcement agencies need a legal basis to exercise their investigatory powers to assist or obtain information for foreign counterparts that are investigating or engaging in enforcement proceedings against fraudulent or deceptive commercial practices or other unlawful conduct that is substantially similar to those in laws that the assisting consumer protection enforcement agencies enforce. Such authorisation may be provided through domestic enabling legislation or, when desired or required, through an international co-operation agreement. Such a legislative basis would allow an agency to remove or reduce barriers to responding to information requests from a foreign agency, but would not result in any unilateral change to foreign or international laws or agreements.

Consumer protection enforcement agencies that are so authorised may decline to co-operate with foreign counterparts on particular investigations or proceedings, or limit or condition such co-operation, on the ground that they consider compliance with a request for co-operation to be inconsistent with their laws, interests or priorities, or resource constraints, or based on the absence of a mutual interest in the investigation or proceeding in question.

Guiding principle 3. Application of investigatory powers to foreign businesses

Principles for Cross-border Enforcement Co-operation for Consumer Protection from OECD Recommendations

The 2003 Cross-border Fraud Recommendation states that Adherents should provide for "Effective mechanisms to adequately investigate, preserve, obtain and share relevant information and evidence relating to occurrences of fraudulent and deceptive commercial practices." (Part II, A, 2)

The 2016 E-commerce Recommendation provides that Adherents should "Establish and maintain consumer protection enforcement authorities that have the authority and powers to investigate and take action to protect consumers against fraudulent, misleading or unfair commercial practices [and] Work towards enabling their consumer protection enforcement authorities to . . . take action against foreign businesses engaged in fraudulent and deceptive commercial practices against domestic consumers." (Part Two, Para 53 (iii)-(iv)). It also provides that Adherents should "Improve the ability of consumer protection enforcement authorities and other relevant authorities, as appropriate, to co-operate and co-ordinate their investigations and enforcement activities, through notification, information sharing, investigative assistance and joint actions." (Part Three, Para 54 (ii)).

[See also UN Guidelines for Consumer Protection, paragraphs V.A. 15, V.I.; 79 (a), 88, 90.]

To implement the above recommendations, consumer protection enforcement agencies should be enabled through domestic legislation to exercise sufficient investigatory powers when businesses under investigation or subject to enforcement proceedings for unlawful practices harming domestic consumers are located overseas. This could include some or all of the following types of domestic legal authority: (i) the authority to seek information voluntarily from foreign businesses or persons; (ii) the authority to seek evidence under any applicable international or regional agreement or convention; (iii) the authority to seek co-operation in obtaining information directly from the foreign consumer protection authority or other regulatory, judicial, or law enforcement authorities, as appropriate; and (iv) the authority to seek information from foreign businesses or persons by other means not prohibited by the foreign country's law.

In developing domestic legislation, countries should also consider how to mitigate, in the context of cross-border enforcement co-operation between governmental consumer protection authorities, the effect of domestic laws that (i) preclude businesses or persons based in their jurisdiction from complying voluntarily with an information request from a consumer protection enforcement agency in a different jurisdiction, when the businesses or individuals direct their activities towards consumers in the requesting authority's jurisdiction, or (ii) prohibit or preclude the foreign enforcement authority from providing assistance to the consumer protection authority seeking such information. Such an approach would not preclude a business or person based in the foreign jurisdiction from invoking protective measures when appropriate.

To implement the above recommendations, consumer protection enforcement agencies should be enabled through domestic legislation to provide assistance to foreign counterparts by obtaining information from domestic businesses and individuals, in appropriate circumstances. A consumer protection agency concerned would assist its foreign counterpart's investigation through the exercise of its existing powers to obtain information, as would be the case for its own investigations. This could permit, but not require, the requested agency to commence formal judicial or administrative proceedings in the jurisdiction where the information is located or otherwise available.

Area II: Enforcement outcomes

Guiding principle 4. Enforcement powers to protect domestic consumers from foreign businesses

Principles for Cross-border Enforcement Co-operation for Consumer Protection from OECD Recommendations

The 2003 Cross-border Fraud Recommendation states that Adherents should "work toward enabling their consumer protection enforcement agencies to take action against foreign businesses engaged in fraudulent and deceptive commercial practices against their own consumers." (Part V, C)

The 2016 E-commerce Recommendation provides that Adherents should work towards enabling their consumer protection enforcement agencies "to take action against foreign businesses engaged in fraudulent and deceptive commercial practices against domestic consumers" (Part Two, Para 53 (iv)).

In addition, the 2007 Dispute Resolution and Redress Recommendation provides that Adherents should work to improve cross-border redress mechanisms including "[d]eveloping multi-lateral and bi-lateral arrangements to improve international judicial co-operation in the recovery of foreign assets and the enforcement of judgments in appropriate cross-border cases."

[See also UN Guidelines for Consumer Protection, Paragraphs V.A. 15, V.I.; 79 (a), 88, 90.]

To implement the above recommendations, consumer protection enforcement agencies should be enabled through domestic legislation to have the legal authority to take action against foreign businesses and persons engaged in fraudulent and deceptive commercial practices and other unlawful conduct that targets and harms domestic consumers. This could include some or all of the following types of domestic legal authority, as appropriate: (i) the authority to investigate or bring actions against a foreign business or person in courts or administrative bodies of their own jurisdiction; (ii) the authority to bring actions against a foreign business or person in the courts of the foreign business's jurisdiction; (iii) the authority to seek co-operation from consumer protection enforcement agencies and other law enforcement authorities in the jurisdiction of the foreign business or person; (iv) the authority to seek measures that could be validly enforced against the foreign businesses concerned, under an applicable international or regional agreement or convention; and (v) the authority to take other actions against foreign businesses or persons by other means not prohibited by the foreign country's law. In developing such legislation, countries should respect relevant principles of international law.

In developing domestic enabling legislation, consumer protection enforcement agencies - directly or by recourse to other authorities or by application to courts or administrative bodies - could seek authorisation to enforce orders providing for redress, whether in the form of monetary payments or conduct remedies, against the overseas business, pursuant to the foreign country's laws on recognition and enforcement of foreign judgments or any applicable international or regional agreement or convention. This may include providing consumer protection authorities with the ability to negotiate and conclude, or otherwise take advantage of, multi-lateral and bi-lateral arrangements to improve international judicial co-operation in the recovery of foreign assets and the enforcement of judgments, in appropriate cross-border consumer protection matters.

Guiding principle 5. Enforcement powers to protect foreign consumers from domestic businesses

Principles for Cross-border Enforcement Co-operation for Consumer Protection from OECD Recommendations

The 2003 Cross-border Fraud Recommendation states that Adherents should "work toward enabling their consumer protection enforcement agencies to take action against domestic businesses engaged in fraudulent and deceptive commercial practices against foreign consumers." (Part V, B)

The 2016 E-commerce Recommendation provides that Adherents should "Work towards enabling their consumer protection enforcement authorities to take action against domestic businesses engaged in fraudulent and deceptive commercial practices against foreign consumers" (Part Two, Para 53 (iv)).

[See also UN Guidelines for Consumer Protection, Paragraphs V.A. 15, V.I.; 79 (a), 88, 90.]

To implement the above recommendations, consumer protection enforcement agencies should be enabled through domestic legislation to have the legal authority to investigate and take action against domestic businesses and persons engaged in fraudulent and deceptive commercial practices and other unlawful conduct targeting and harming foreign consumers. This could include some or all of the following types of domestic legal authority, as appropriate: (i) the authority to investigate or take enforcement measures and/or bring actions against a domestic business or person before domestic courts or administrative bodies, and (ii) the authority to seek co-operation from consumer protection enforcement agencies and other law enforcement authorities in the jurisdiction of the foreign consumers to seek information and evidence. In developing such legislation, countries should respect relevant principles of international law while seeking to avoid creating regulatory or enforcement gaps that allow businesses to deceive or otherwise harm consumers by taking advantage of national borders.

Guiding principle 6. Minimum enforcement outcomes

Principles for Cross-border Enforcement Co-operation for Consumer Protection from OECD Recommendations

The 2003 Cross-border Fraud Recommendation states that Adherents should provide for "Effective mechanisms to adequately investigate, preserve, obtain and share relevant information and evidence relating to occurrences of fraudulent and deceptive commercial practices" (Part II, A, 2) and "Effective mechanisms to stop businesses and individuals engaged in fraudulent and deceptive commercial practices" (Part II, A, 3). It further states that consumer protection enforcement agencies "whose territories are affected by fraudulent and deceptive commercial practices against consumers should have appropriate authority to investigate and take action within their own territory." (Part V, A)

The 2016 E-commerce Recommendation provides that Adherents should "Establish and maintain consumer protection enforcement authorities that have the authority and powers to investigate and take action to protect consumers against fraudulent, misleading or unfair commercial practices and the resources and technical expertise to exercise their powers effectively" (Part Two, Para 53 (iii). It also provides that Adherents should "Improve the ability of consumer protection enforcement authorities and other relevant authorities, as appropriate, to co-operate and co-ordinate their investigations and enforcement activities, through notification, information sharing, investigative assistance and joint actions" (Part Three, Para 54 (ii)).

[See also UN Guidelines for Consumer Protection, Paragraphs V.A. 15, 37-41; V.I.; 79 (a), 88, 90.]

To implement the above recommendations, consumer protection enforcement agencies should be enabled through domestic legislation to have the legal authority to obtain, either directly or through the application to courts or administrative tribunals, effective enforcement outcomes, including but not limited to:

a. Permanent injunctive orders to prevent, stop, or change business conduct. These orders may include the power to require businesses to take positive steps that may go beyond strict legal requirements in certain circumstances, such as through a negotiated settlement order, to the extent permitted by domestic law.
b. Temporary or preliminary injunctive orders to prevent, stop or change harmful business conduct before a final adjudication.
c. Statutory penalties or fines in appropriate cases, in particular to correct delays by businesses coming into compliance or failing to adhere to promises to change, and where calculation of individual loss is impractical or disproportionate.
d. Redress, including when appropriate, monetary redress for consumers who have suffered economic harm. There are many different mechanisms for consumer protection authorities to obtain or facilitate redress on behalf of consumers. These include, but are not limited to:
    i. The ability to seek a court order for redress in civil proceedings.
    ii. The ability to seek a court order for redress in criminal proceedings.
    iii. The ability to act as a representative party in lawsuits seeking redress.
    iv. The ability to seek to obtain commitments from the trader to offer adequate remedies to the consumers that have been affected by that infringement. Where appropriate, in seeking such remedies, consumer protection enforcement agencies may be assisted by other enforcement entities such as private consumer organisations.

v. Statements to be published by businesses to publicise the outcome of enforcement as well as to correct their misleading presentations.

vi. Orders requiring third parties to cease providing services (including website and social media profile takedowns, payment services, and delivery disruption).

vii. Recovery of business assets to ensure compliance or secure monetary redress.

Area III: Co-operation practices

Guiding principle 7. Notification and alerts

Principles for Cross-border Enforcement Co-operation for Consumer Protection from OECD Recommendations

The 2003 Cross-border Fraud Recommendation states that Adherents and their consumer protection enforcement agencies should "develop ways to promptly, systematically and efficiently notify consumer protection enforcement agencies in other Member countries of investigations that affect those countries, so as to alert them of possible wrongdoing in their jurisdiction, simplify assistance and co-operation under these Guidelines and avoid duplication of efforts and potential disputes." (Part IV, A). It further states that Adherents should "strive to improve the abilities of consumer protection enforcement agencies to share information within timeframes that facilitate investigations of matters involving fraudulent and deceptive commercial practices against consumers, subject to appropriate safeguards" (Part IV, B).

The 2016 E-commerce Recommendation provides that Adherents should "Improve the ability of consumer protection enforcement authorities and other relevant authorities, as appropriate, to co-operate and co-ordinate their investigations and enforcement activities, through notification, information sharing, investigative assistance and joint actions" (Part Three, Para 54 (ii)).

[See also UN Guidelines for Consumer Protection, Paragraphs V.A. 15, V.I.; 79 (a), 82, 88, 90.]

To implement the above recommendations, consumer protection enforcement agencies should be enabled through domestic legislation to have the legal authority to notify foreign counterparts of possible wrongdoing, including by providing the relevant information. This should include the ability to share details about businesses and associated individuals under investigation, as well as the existence of an agency investigation. In doing so, consumer protection agencies should act in accordance with applicable law on privacy, data security, and confidentiality, including any laws or rules governing the sharing or transferring information containing personal data with foreign administrative or enforcement authorities.

Consumer protection enforcement agencies should be enabled through domestic legislation to have the legal authority to alert foreign counterparts of emerging risks, co-ordinate on potential investigative enforcement priorities and opportunities for co-operation, simplify assistance procedures, and avoid conflicts and duplication of efforts.

Guiding principle 8. Information and evidence sharing

Principles for Cross-border Enforcement Co-operation for Consumer Protection from OECD Recommendations

The 2003 Cross-border Fraud Recommendation states that Adherents should provide for "Effective mechanisms to adequately investigate, preserve, obtain and share relevant information and evidence relating to occurrences of fraudulent and deceptive commercial practices." (Part IV, A). It further states that Adherents should "work towards enabling their consumer protection enforcement agencies to share the following information with consumer protection enforcement agencies in other Member countries in appropriate instances:

1. Publicly available and other non-confidential information.
2. Consumer complaints.
3. Information about addresses, telephones, Internet domain registrations, basic corporate data, and other information permitting the quick location and identification of those engaged in fraudulent and deceptive commercial practices.
4. Expert opinions, and the underlying information on which those opinions are based. And
5. Documents, third-party information, and other evidence obtained pursuant to judicial or other compulsory process" (Part IV, B).

The 2016 E-commerce Recommendation provides that Adherents should "Improve the ability of consumer protection enforcement authorities and other relevant authorities, as appropriate, to co-operate and co-ordinate their investigations and enforcement activities, through notification, information sharing, investigative assistance and joint actions" (Part Three, Para 54 (ii)).

To implement the above recommendations, consumer protection enforcement agencies should be enabled through domestic legislation to have the legal authority to share information relevant to possible wrongdoing with foreign counterparts. In doing so, consumer protection agencies should act in accordance with applicable law on privacy, data security, and confidentiality, including any laws or rules governing the sharing or transferring of information containing personal data with foreign administrative or enforcement authorities. Such information could include:

a. The details of consumer complaints, including personal data when appropriate.
b. Information about specific businesses, including confidential information about a business or other information about the business obtained pursuant to judicial or other compulsory process from the businesses or a third party.
c. Expert opinions, and the underlying information on which those opinions are based.
d. Information on whereabouts, addresses, associated telephone numbers and other electronic means of contact, Internet domain registrations, as well as appropriate domain name registration information for websites that are promoting or engaging in commercial transactions with consumers.

Guiding principle 9. Confidentiality

Principles for Cross-border Enforcement Co-operation for Consumer Protection from OECD Recommendations

The 2003 Cross-border Fraud Recommendation states that Adherents should "take appropriate steps to maintain the necessary confidentiality of information exchanged under these Guidelines, in particular in sharing confidential business or personal information." It further states that Adherents should "respect safeguards requested by other Member countries to protect confidential business or personal information shared with them" (Part IV, F).

The 2016 E-commerce Recommendation provides that Adherents should "Strive to improve the ability of consumer protection enforcement authorities to share information subject to appropriate safeguards for confidential business information or personal data" (Part Three, Para 54 (ii)).

To implement the above recommendations, when consumer protection enforcement agencies share information with foreign counterparts, the recipient of the information should have the legal authority to keep both the information and the related investigation confidential, and be required to use the information obtained only for official law enforcement purposes. The information should be treated as confidential and should only be used and disclosed with due regard to the commercial interests of a natural person or legal person, including trade secrets and intellectual property.

The recipient of the information should have the ability to limit the use of the information to the purpose for which it was shared. Laws or other rules requiring the recipient to make information they hold public would provide suitable exemptions for information supplied by foreign counterparts who request it to remain confidential and suitable rules on the disclosure of such information in formal enforcement proceedings.

Consumer protection enforcement agencies should return or delete any information that is no longer needed for an investigation or in formal enforcement proceedings, using secure methods, as soon as practicable. If this is not feasible, consumer protection enforcement agencies should maintain the confidentiality of any information received from foreign counterparts that has not been made public during enforcement proceedings when the agency providing the information has requested confidential treatment as a condition of providing the information. When this is not possible, agencies should make this clear to potential co-operating authorities before the information is shared to avoid inadvertent disclosure.

Sharing and handling of personal data can only be done under the conditions and safeguards provided by applicable laws on the protection of personal data. In general, personal data should be deleted, or rendered anonymous, once the purpose of handling or processing has been achieved.

Guiding principle 10. Co-ordination of investigations and outcomes

Principles for Cross-border Enforcement Co-operation for Consumer Protection from OECD Recommendations

The 2003 Cross-border Fraud Recommendation states that consumer protection enforcement agencies should "co-ordinate their investigations and enforcement activity to avoid interference with the investigations and enforcement activity of consumer protection enforcement agencies taking place in other Member countries" (Part III, B). It further states that consumer protection enforcement agencies should "make every effort to resolve disagreements as to co-operation that may arise" (Part III, C).

The 2016 E-commerce Recommendation provides that Adherents should "Simplify assistance and co-operation, avoid duplication of efforts, and make every effort to resolve disagreements as to co-operation that may arise, recognising that co-operation on particular cases or investigations remains within the discretion of the consumer protection enforcement authority being asked to co-operate" (Part Three, Para 54 (ii)).

To implement the above recommendations, consumer protection enforcement agencies should be enabled through domestic legislation to have the legal authority to co-ordinate their investigations and discuss potential outcomes with foreign counterparts in accordance with what is permitted by domestic rules on confidentiality and privacy and data protection. Rules on confidentiality or process should provide for sufficient gateways or mechanisms for appropriate discussions to take place, even if these may require the counterpart to give assurances as to confidentiality.

Consumer protection enforcement agencies should make every effort to co-ordinate their investigations and enforcement activities to avoid interference with the investigations and enforcement activities of foreign consumer protection enforcement agencies. Consumer protection enforcement agencies should make every effort to resolve disagreements as to co-operation that may arise.

Consumer protection enforcement agencies working in parallel should, when appropriate, aim to secure outcomes that are consistent overall, taking into consideration differences in agency structure, powers, and applicable law. This could involve several consumer protection authorities agreeing a common position as to what outcomes they can achieve under their own law, and using this as the basis for their approach to businesses under investigation. Depending on the compatibility of legal regimes, the participating authorities could also appoint a lead authority to co-ordinate the co-operation.

Annex. Detailed guide

Area I: Investigatory powers

Guiding principle 1: Domestic investigatory powers

> The 2003 Cross-border Fraud Recommendation states that Adherents should provide for "Effective mechanisms to adequately investigate, preserve, obtain and share relevant information and evidence relating to occurrences of fraudulent and deceptive commercial practices" (Part II, A, 2).
>
> The 2016 E-commerce Recommendation provides that Adherents should "Establish and maintain consumer protection enforcement authorities that have the authority and powers to investigate and take action to protect consumers against fraudulent, misleading or unfair commercial practices and the resources and technical expertise to exercise their powers effectively" (Part Two, Para 53 (iii)).

Sources: 2003 Cross-Border Fraud Recommendation, Part II, A, 2; 2016 E-commerce Recommendation Part Two, Para 53 (iii); also relevant to UN Guidelines for Consumer Protection, Paragraphs V.A. 15, V.I.; 79 (a), 88.

Rationale

There are three key reasons why consumer protection enforcement agencies should consider a comprehensive set of investigatory powers.

The first is to ensure operational effectiveness. An agency that is not able to investigate businesses' practices within its jurisdiction may struggle to hold those businesses to account, with the result that investigations may take an excessive length of time to complete, or the business is able to continue infringing the law. This may result in consumers being harmed, fair dealing competitors being disadvantaged, and the rule of law being undermined. A comparison of investigatory powers held by consumer protection enforcement agencies across the globe reveals that some agencies are better equipped than others; therefore, this guide aims to set out the essential powers that any consumer protection enforcement agency needs to be effective.

The second is to ensure powers that are fit for the digital age. Increasingly evidence is held on electronic devices, which may be located away from the premises of the business under investigation (for example where cloud storage is used), and which may require the active co-operation of the business to access in a way that accessing documents held in a filing cabinet does not. Likewise, conducting a test purchase online is practically different to making a purchase in a shop. Aside from the practicalities, discovering the identity of online businesses and accessing digital data may engage rules on privacy and data protection that require careful consideration. Accordingly, legislators engaged in developing or amending consumer protection laws might consider providing appropriate safeguards that enable consumer protection enforcement agencies to investigate effectively while safeguarding citizens' legitimate privacy interests.

Finally, businesses increasingly operate in multiple jurisdictions. For example, a business selling to consumers in the United Kingdom may operate its website from Spain, with data held on servers in

Panama, customer complaints handled in Ireland and an overall head office in the United States. In order to investigate alleged consumer harm, it is likely to be necessary to access evidence in all of these jurisdictions. However, this becomes very difficult if a consumer protection enforcement agency in one of those jurisdictions is not able to obtain the relevant evidence because they lack the power.

Detail of the powers

In devising an investigative toolkit, the legislator needs to strike a balance between conferring on consumer protection enforcement agencies the means to maintain a high level of consumer protection, through effective enforcement, and safeguarding civil liberties and freedoms, such as the right to privacy. This section sets out what each power would ideally achieve and any particular safeguards that should be considered.

Information gathering

Consumer protection enforcement agencies can usefully be empowered by requiring the provision of information, both by businesses under investigation, and third parties who may have relevant information.

Information that a consumer protection enforcement agency may require could include:

a. Documents, digital data and other information already in existence, irrespective of the storage medium or the place where they are stored, to be produced in a form which the consumer protection enforcement agency can read.

b. The creation of new documents, digital data and other information.

c. Testimonial evidence, including any information relevant to the alleged infringement; explanations of documents or data provided; explanations of decisions taken, and the intentions and motivations for doing so.

d. Information relating to financial and data flows, the identity of persons involved in financial and data flows, including the information necessary to ascertain bank account information and ownership of websites and other accounts.

Some safeguards likely to be considered appropriate include:

a. Withholding information that is covered by an applicable legal professional privilege (and if no exceptions to that privilege apply).

b. Providing the recipient of the information request with a legal basis to assert protections against self-incrimination when the information may be used in criminal proceedings.

c. Limiting information requests to documents, testimony, or other information that is relevant to the investigation of the alleged infringement. In some jurisdictions, consumer protection enforcement agencies may be required to show that the information is reasonably necessary and proportionate.

d. Providing clear instructions in the information request about what information is required, the manner in which it is to be provided and the date by which it is due.

Preservation of evidence

Countries might consider whether their consumer protection enforcement agencies should have some mechanism to require persons to preserve evidence, particularly that of a transient nature, in particular investigations, until it can be examined. This could include ensuring that data is not automatically deleted, or that cloud storage can continue to be accessed from specific premises.

Enforcement of information requests

Countries might wish to consider whether their consumer protection enforcement agencies should be able to compel the production by a business of relevant information, either administratively or judicially. This power could usefully be used where a person has failed or refused to respond to an information request (within the required time or in the required manner) and where a person has provided false or misleading information to the consumer protection enforcement agency. Generally speaking, persons who fail to comply with an administrative or judicial order should face effective, proportionate and dissuasive sanctions.

Undercover investigations

Countries might wish to consider whether their consumer protection enforcement agencies may simulate the consumer's experience of dealing with a business, to test the extent to which the business complies with the law. This is known as 'test purchasing' or 'mystery shopping' in some jurisdictions.

The activities that consumer protection enforcement agencies might usefully be able to carry out include:

a. Obtaining any product, including personalised services such as loans, whether or not it involves spending money.
b. Subscribing to any distribution list or closed customer group.
c. Carrying out any step that could lead to a purchase of a product.
d. Monitoring any information put into the public domain about a business.
e. Recording the activity.

In order to conduct effective test purchases, consumer protection enforcement agencies may need to have access to covert payment cards, delivery addresses and means of communication so that they are able to conceal their identity as enforcement officers.

Safeguards could include ensuring individual staff members are not liable under contracts they enter into when conducting a test purchase, and that such contracts may be cancelled within a reasonable time. In the event of cancellation, any items purchased should be returned to the business, unless required as evidence.

Because a covert test purchase may involve risks to the officer who conducts it, as well as potentially interfering with the business's right to privacy, such activity could be carried out only by appropriately trained staff who are authorised by a more senior officer. The activity could be carried out only when necessary and proportionate, and collateral interference with the privacy of the business or any other persons should be minimised.

Observing the conduct of business

Countries might consider whether their consumer protection enforcement agency should be able to inspect how a business under investigation engages in their commercial practices. In some jurisdictions this could require authorisations by a court or administrative tribunal. Particular activities could include:

a. Observing a business's interaction with another consumer (either covertly, for example by attending a doorstep sale or overtly, for example by listening in to telesales calls in accord with relevant law e.g. privacy or wiretapping provisions).
b. Visiting premises open to the public to observe practices such as shelf labelling or to check who occupies the premises.
c. Inspecting or otherwise obtaining information about business operations and processes relevant to any prohibitions.

Similar safeguards apply as to undercover investigations.

Entry to premises

Countries might consider whether their consumer protection enforcement agencies should be able in appropriate cases to access business premises (including vehicles), in order to be able to gather evidence of suspected infringing conduct, which is either on those premises or accessible from those premises. The following powers would ideally be available, subject to appropriate conditions (which, depending on the circumstances and the jurisdiction, include court approval):

a. Entry to business premises without notice, where there is reason to believe that giving notice would defeat the purpose of the entry, or the occupier of the premises agrees to the entry.

b. Entry to premises on reasonable notice for compliance purposes.

c. Entry to business premises where access to the premises has been or is likely to be refused (or the premises are unoccupied), or it is likely that evidence accessible on or from the premises would be concealed or interfered with if notice were given. A judicial warrant should empower the consumer protection enforcement agency to search the premises and secure evidence, as described below.

Obtaining evidence

Countries might consider whether their consumer protection enforcement agencies should be able to access and copy relevant evidence of a business's practices, including digital evidence, irrespective of the storage medium or the place where the evidence is stored. In order to access evidence, the consumer protection enforcement agency would ideally be able to compel production of the evidence, or enter premises, under the conditions described above. In the case of digital evidence, the consumer protection enforcement agency could be enabled by domestic legislation to require production of passwords or other security keys.

Assistance

Consumer protection enforcement agencies could also be enabled to require assistance and explanations from persons present on the inspected (or searched) premises. This is so that inspections can take place as efficiently as possible, and also so that consumer protection enforcement agencies can secure evidence which is hard to find or access, such as data held in password protected files or on foreign servers only accessible by means of an electronic key.

Sanctions for obstruction

Effectively obtaining evidence from a legal or natural person, whether by demands to produce evidence or by inspection, would usefully require that person or their staff to co-operate, and provide reasonable assistance. Where instead they put obstacles in the way of the investigation, mislead the investigator or refuse to provide information reasonably required, they should be subject to effective, proportionate and dissuasive sanctions. Such sanctions could include an administrative fine or even criminal prosecution. The legislation may include a threshold of knowledge, recklessness or intention to obstruct, as a safeguard.

Domestic coordination

Domestic enforcement can be enhanced when different domestic authorities are able to exchange details and evidence regarding investigative targets. This can result in parallel cases with, for example, safety and health regulators involving unsafe or unproven products, with telecommunications providers for unauthorised charges on consumers' financial, telephone or other accounts, or referrals to criminal enforcement authorities in matters involving fraud. See 2003 Cross-Border Fraud Recommendation, Part IV, C.

I. Case examples

Sweden

The Swedish Consumer Agency ("the Agency") has made use of mystery shopping in a number of cases. For example, a company claimed that a non-compliant life jacket marketed on its website was not sold to consumers. Through mystery shopping the Agency was able to prove that the jacket was indeed being sold to consumers. In an investigation into a dustpan the Agency suspected had very sharp and potentially unsafe metal edges, the Agency requested a sample of the dustpan from the manufacturer. The sample provided by the manufacturer appeared to be a "golden sample", where the sharp edges had been manually filed. Through mystery shopping, involving the Agency purchasing the same product through another channel, the Agency was able to obtain an unaltered sample – which indeed had very sharp edges. Finally, the Agency has also undertaken concealed test purchases of pram accessories which the Agency suspected deviated from current standards.

United States

Undercover investigations – The United States (US) Federal Trade Commission (FTC) has developed and utilised a variety of undercover techniques to investigate and prosecute consumer fraud cases, as well as to obtain redress and other relief for injured consumers. For example, FTC staff investigators sometimes pose as consumers and purchase a product on a website or sign up for a service promoted by a telemarketer. The investigator stands in the shoes of consumers, observes the conduct consumers observe, and gathers evidence of possible law violations. The interactions captured by FTC investigators often provide the most probative and accurate evidence of how a business actually treats consumers, exposing deceptive and unfair practices that might otherwise go undetected or unprosecuted. Courts have recognised and relied on this evidence in a wide variety of cases. FTC attorneys play an important oversight role in the collection of evidence from undercover operations by, for example, advising investigators about the relevant state and federal statutes governing the recording of telephone or live interactions and ensuring investigators not to cross the line between capturing and instigating a law violation. FTC attorneys operate under various state professional responsibility licensing rules and all FTC employees operate under federal ethics laws and regulations. The agency also uses undercover techniques in certain industry-wide investigations, such as in its periodic inspections of funeral homes to assess compliance with the FTC's Funeral Rule, which requires funeral homes to provide itemised information to consumers about the price of funeral goods and services.

Domestic coordination – The US FTC routinely brings enforcement actions with domestic partners at the federal and state level. For example, the FTC coordinated with the US Consumer Financial Protection Bureau and the US Federal Communications Commission (FCC) as well as state attorneys general on a series of law enforcement actions against wireless carriers for allowing unauthorised third-party charges on consumers' telephone bills, a practice known as mobile cramming. In one of those cases, involving wireless carrier T-Mobile USA, Inc., the company agreed to fully refund its customers for unwanted third-party charges it placed on their phone bills, paying at least USD 90 million (United States dollars) to settle a FTC lawsuit. In addition to providing the full refunds, T-Mobile paid USD 18 million in fines and penalties to the attorneys general of all 50 states and the District of Columbia and USD 4.5 million to the FCC. The settlement also required the company to get consumers' express informed consent before placing third-party charges on their bill and ensure consumers are provided with information about blocking third-party charges. In another action that also involved the FCC and the states, AT&T Mobility LLC agreed to pay USD 105 million, including USD 80 milllion for refunds, and to notify customers who were billed for unauthorised third-party charges of the refund program. Under the settlement, the company also significantly changed its process for third-party billing.

II. Statutory examples

European Union

Under Article 9, paragraph 3 of Regulation(EU) 2017/2394 of the European Union (the Consumer Protection Co-operation or CPC Regulation), which establishes a set of minimum investigation and enforcement powers for consumer protection and enforcement authorities within the EU, such authorities shall have at least the following investigation powers:

> (a) the power of access to any relevant documents, data or information related to an infringement covered by this Regulation, in any form or format and irrespective of their storage medium, or the place where, they are stored
>
> (b) the power to require any public authority, body or agency within their Member State or any natural person or 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
>
> (c) the power to carry out necessary on-site inspections, including the power to enter any premises, land or means of transport that the trader concerned by the inspection uses for purposes related to his trade, business, craft or profession, or to request other public authorities to do so, in order to examine, seize, take or obtain copies of information, data or documents, irrespective of their storage medium; the power to seize any information, data or documents for a necessary period and to the extent necessary for the inspection; the power to request any representative or member of the staff of the trader concerned by the inspection to give explanations of facts, information, data or documents relating to the subject matter of the inspection and to record the answer
>
> (d) the power to purchase goods or services as test purchases, where necessary, under a cover identity, in order to detect infringements covered by this Regulation and to obtain evidence, including the power to inspect, observe, study, disassemble or test goods or services.

Under Article 29 of the CPC Regulation, which sets out the general rules for conducting sweeps by EU and EEA (European Economic Area) national competent authorities:

> 1. The competent authorities may decide to conduct sweeps to check compliance with, or to detect infringements of Union laws that protect consumers' interests. Unless otherwise agreed upon by the competent authorities involved, sweeps shall be coordinated by the Commission.
>
> 2. When conducting sweeps, the competent authorities involved may use the investigation powers set out in Article 9(3) and any other powers conferred upon them by national law.
>
> 3. The competent authorities may invite designated bodies, Commission officials, and other accompanying persons authorised by the Commission, to participate in sweeps.

United Kingdom

Schedule 5 (in particular paragraphs 14-18 and 21-36) of the United Kingdom's Consumer Rights Act 2015, provides a number of specific powers to United Kingdom (UK) enforcers, including to require the production of information and to take action to enforce it, to test purchase and to conduct on-site inspections:

> Power to require the production of information
>
> 14 An enforcer or an officer of an enforcer may give notice to a person requiring the person to provide the enforcer with the information specified in the notice.

Power to purchase products

21(1) An officer of an enforcer may—

(a) make a purchase of a product, or

(b) enter into an agreement to secure the provision of a product.

(2) For the purposes of exercising the power in sub-paragraph (1), an officer may—

(a) at any reasonable time, enter premises to which the public has access (whether or not the public has access at that time), and

(b) inspect any product on the premises which the public may inspect.

(3)The power of entry in sub-paragraph (2) may be exercised without first giving notice or obtaining a warrant.

Power to observe carrying on of business etc.

22(1) An officer of an enforcer may enter premises to which the public has access in order to observe the carrying on of a business on those premises.

(2) The power in sub-paragraph (1) may be exercised at any reasonable time (whether or not the public has access at that time).

(3) The power of entry in sub-paragraph (1) may be exercised without first giving notice or obtaining a warrant.

Power to enter premises without warrant

23(1) An officer of an enforcer may enter premises at any reasonable time.

(2) Sub-paragraph (1) does not authorise the entry into premises used wholly or mainly as a dwelling.

(3) In the case of a routine inspection, the power of entry in sub-paragraph (1) may only be exercised if a notice has been given to the occupier of the premises in accordance with the requirements in sub-paragraph (4), unless sub-paragraph (5) applies.

(4) Those requirements are that—

(a) the notice is in writing and is given by an officer of the enforcer,

(b) the notice sets out why the entry is necessary and indicates the nature of the offence under paragraph 36 (obstruction), and

(c) there are at least two working days between the date of receipt of the notice and the date of entry.

(5) A notice need not be given if the occupier has waived the requirement to give notice.

United States

The US Federal Trade Commission Act provides the US FTC with a number of investigative powers, including the power to issue a civil investigative demand (CID) to obtain documents or oral testimony in an investigation of possible “unfair or deceptive acts or practices” (Federal Trade Commission Act section 20, 15 U.S.C. Sec. 57b-1). A CID also requires that the recipient “file written reports or answers to questions” (15 U.S.C. Sec. 57b-1(c)(1)). In addition, section 20 expressly authorises the issuance of CIDs requiring the production of tangible things and provides for service of CIDs upon entities not found within the territorial jurisdiction of any court of the United States (15 U.S.C. Sec. 57b-1(c)(7)(B)). Rule 2.7 of the FTC’s Rules of Practice, codified in the Code of Federal Regulations (C.F.R.), specifies the four main types

of information the FTC may obtain via CID – documents, tangible things, reports or written answers to questions, and oral testimony- and the procedures for doing so as follows:

> (1) CIDs for the production of documentary material, including ESI (electronically stored information), shall describe each class of material to be produced with sufficient definiteness and certainty as to permit such material to be fairly identified, prescribe a return date providing a reasonable period of time within which the material so demanded may be assembled and made available for inspection and copying or reproduction, and identify the Commission's custodian to whom such material shall be made available.
>
> (2) CIDs for tangible things, including electronic media, shall describe each class of tangible thing to be produced with sufficient definiteness and certainty as to permit each such thing to be fairly identified, prescribe a return date providing a reasonable period of time within which the things so demanded may be assembled and submitted, and identify the Commission's custodian to whom such things shall be submitted.
>
> (3) CIDs for written reports or answers to questions shall propound with sufficient definiteness and certainty the reports to be produced or the questions to be answered, prescribe a return date, and identify the Commission's custodian to whom such reports or answers to questions shall be submitted.
>
> (4) CIDs for the giving of oral testimony shall prescribe a date, time, and place at which oral testimony shall commence, and identify the hearing official and the Commission custodian. Oral testimony in response to a CID shall be taken in accordance with the procedures set forth in section 20(c)(14) of the Federal Trade Commission Act.

Other provisions of the C.F.R. set out safeguards such as notice of the purpose of the investigation (16 CFR § 2.6) and the rights of witnesses in investigations (16 C.F.R. § 2.9) and procedures and bases for withholding requested material (16 C.F.R. § 2.11).

Further provisions of the C.F.R. (16 C.F.R. § 4.11, paragraphs (b) and (c)) permit the FTC to share information with federal and state agencies.

Guiding principle 2: Application of investigatory powers to assist foreign consumer protection enforcement agencies

The 2003 Cross-border Fraud Recommendation states that Adherents should improve "their ability to co-operate in combating cross-border fraudulent and deceptive commercial practices recognising that co-operation on particular investigations or cases under these Guidelines remains within the discretion of the consumer protection enforcement agency being asked to co-operate." It further states that the agency may "decline to co-operate on particular investigations or proceedings, or limit or condition such co-operation, on the ground that it considers compliance with a request for co-operation to be inconsistent with its laws, interests or priorities, or resource constraints, or based on the absence of a mutual interest in the investigation or proceeding in question" (Part III, A). It further provides that Adherents should "work toward authorising their consumer protection enforcement agencies, either directly or through appropriate mechanisms authorised by their judicial or administrative authorities, to obtain information, including documents and statements, and otherwise provide investigative assistance for foreign consumer protection enforcement agency investigations and actions, subject to appropriate safeguards" (Part IV, D).

The 2016 E-commerce Recommendation provides that Adherents should "Improve the ability of consumer protection enforcement authorities and other relevant authorities, as appropriate, to co-operate and co-ordinate their investigations and enforcement activities, through notification, information sharing, investigative assistance and joint actions." In particular, it provides that Adherents should "Simplify assistance and co-operation, avoid duplication of efforts, and make every effort to resolve disagreements as to co-operation that may arise, recognising that co-operation on particular cases or investigations remains within the discretion of the consumer protection enforcement authority being asked to co-operate" (Part Three, Para 54 (ii)).

Sources: 2003 Cross-Border Fraud Recommendation, Part III, A, IV, D; 2016 E-commerce Recommendation Part Three, Para 54 (ii); also relevant to UN Guidelines for Consumer Protection, Paragraph VI.83, 88, 90.

Rationale

In many consumer protection investigations and cases, the evidence that a consumer protection enforcement agency needs for its investigation may be located in a different jurisdiction. Although the consumer protection enforcement agency can try to obtain the information voluntarily from the business, the business may sometimes not be willing to provide the information to the agency without a subpoena or other compulsory process issued by the courts or administrative bodies of the jurisdiction where the business is located. The consumer protection enforcement agency may not be able to use an international agreement or convention, such as a Mutual Legal Assistance Treaty, because either there is no applicable agreement or convention, the alleged law violation is not within its scope, or the process may be too burdensome or slow.

If the consumer protection enforcement agency in the jurisdiction where the evidence is located has the power to provide investigative assistance to the investigating authority, it can obtain the information from the domestic business. In many cases, this can help not only the investigating authority but also the consumer protection authority in the jurisdiction where the business is located because the practice that is being investigated may also be affecting or harming consumers in that jurisdiction. It may also send a strong signal, in the case of multinational companies, that they cannot use national borders to avoid complying with laws. This power is a key component of a culture of mutual assistance that enables consumer protection authorities to achieve greater results working together than they ever could alone.

Examples

I. Case examples

Australia

In 2013, the Australian Competition and Consumer Commission (ACCC) sought formal co-operation with the US FTC through its SAFE WEB Act to access investigative materials and witnesses in relation to the FTC's enforcement action against Reebok International Ltd. The Federal Court of Australia subsequently imposed penalties totalling AUD 350 000 (Australian dollars) against Reebok Australia.

Canada

In 2011, the Competition Bureau Canada (CBC) led an investigation into a business directory scheme targeting Canadian and international businesses. As part of this investigation, the CBC received the support of the US FTC and the ACCC (which also brought their own enforcement actions), as well as the National Fraud Intelligence Bureau of the United Kingdom. The CBC also received the support of ICPEN, and the International Mass Marketing Fraud Working Group (see further details on this case under Guiding principle 4).

In response to a US Postal Inspection Service and US Department of Justice (USPIS-DOJ) request, the CBC shared information obtained through Canada's Competition Act formal powers with the USPIS-DOJ to assist them in an investigation of a fraudulent mailing scheme targeting seniors.

In response to a US FTC request, the CBC shared information obtained through formal powers with the FTC to assist them in an investigation of a matter involving deceptive telemarketing.

European Union

In 2020, in line with the CPC Regulation (see relevant provisions below), the authorities from the EU and EEA submitted 25 requests for information to their counterparts in other EU/EEA countries, in order to establish whether an intra-EU infringement had occurred and if so bring about the cessation of that infringement. 19 of these requests were closed after the requested authorities had provided the information sought.

Turkey

In 2019, in a joint letter the Belgian Directorate General for Economic Inspection (DGEI) and the Netherlands Authority for Consumers and Markets (ACM) requested the assistance from the Turkish Ministry of Trade regarding an investigation into fraudulent debt collecting agencies with ties to two call centres established in Turkey. The Statutory Decree on Organisation and Duties of the Ministry of Customs and Trade provided the Ministry of Trade with power to assist with the information request to a certain degree. The Ministry of Trade communicated with other domestic agencies and departments in order to gain further information requested, and assisted the ACM in particular by: providing the trade registry records of the companies involved - including company names, founders, stakeholders, owners and addresses as well as other commercial entities that the individuals involved in the investigation were related to; informing the ACM about the content of the documents sent by one of the companies to the ACM and revealing the information hidden in those documents; assisting with physical delivery of information; and verifying the open source information collected by the ACM. The ACM was subsequently able to conclude the investigation with the help of the information provided.

United States

In 2018, the US FTC used its SAFE WEB powers to issue six CIDs to US entities associated with Viagogo, a company based in Switzerland, which was the subject of an enforcement action brought by the UK Competition and Markets Authority (CMA) against Viagogo UK (and its Swiss parent) for violating various consumer laws through its advertising and pricing representations. The company produced some

information to the FTC, which the agency shared with the CMA. Before the FTC moved to compel the production of other, responsive information, the CMA secured a court order against Viagogo by consent and the FTC withdrew its CIDs.

In 2014, the US FTC used its SAFE WEB Act powers to apply for an order from a US federal district court on behalf of the CBC under section 1782 of the United States Code. The order permitted the FTC to obtain oral and documentary testimony from Aegis Mobile LLC, a company based in Maryland. Aegis had evidence relevant to the CBC's enforcement action against its three largest wireless carriers and the Canadian Wireless Telecommunications Association (CWTA) for deceptive advertising involving premium text messaging. The CWTA had hired the US company to collect and analyse advertising that was the subject of the CBC's enforcement action.

In 2015, the US FTC further used its SAFE WEB authority to assist the Royal Canadian Mounted Police (RCMP) in its investigation of Banners Brokers, a massive online pyramid scheme based in Canada that targeted consumers around the world. Ultimately, the Toronto Police (working with the RCMP) arrested two of Banners Brokers' three principals and charged them criminally for their participation in the USD 93 million scheme.

Zambia

In 2019, the Zambian Competition and Consumer Protection Commission (CCPC) used the African Dialogue's Principles on Cooperation in Consumer Protection Enforcement, known as the Livingstone Principles (non-binding), to request investigative assistance from the Tanzanian Fair Competition Commission (FCC) via the COMESA Competition Commission. The investigation involved a case against Fast Jet, a Tanzanian airline that operated in Zambia which eventually closed down. The co-operation was necessary to help a consumer get their refund. Fast Jet allegedly cancelled a flight, resulting in the complainant requesting a refund as the complainant could not travel at a later date since his travel was time bound. The Zambian Competition and Consumer Protection Act (CPA) has limited jurisdiction to Zambia. As such, the CCPC could not pursue Fast Jet in Tanzania. The Tanzanian FCC responded that unfortunately, Fast Jet had also closed in Tanzania and hence could not commence investigations against them. In 2019, African Dialogue countries reaffirmed their commitment to using the Livingstone Principles to facilitate cross-border consumer protection enforcement.

Example from the competition area

In November 2014, the Italian competition authority (AGCM) launched an investigation against the pharmaceutical group Aspen EUR 5.2 million for an alleged infringement of Art. 102(a) of the Treaty on the Functioning of the European Union (TFEU), consisting in the imposition of excessive and unfair prices for its off-patent anti-cancer drugs. The investigation concerned inter alia the following undertakings: Aspen Pharma Trading Limited (APTL) and Aspen Pharma Ireland Limited (APIL), both with registered offices in Dublin. The AGCM made a request for investigatory assistance pursuant to Article 22 of Regulation No. 1/2003 to the Irish Competition and Consumer Protection Commission (CCPC). As a result, the CCPC carried out inspections at the premises of APTL and APIL. The documentation gathered by the CCPC during its inspections was subsequently sent to the AGCM, pursuant to Article 12 of Regulation No. 1 /2003 and added to the AGCM case file (OECD & International Competition Network, 2021[5]).

II. Statutory examples

Canada

In Canada, the Competition Act ("the Act") provides for the sharing of information with foreign authorities under certain circumstances. Sections 74.012 and 52.02, known as the foreign assistance provisions, facilitate international assistance with organisations that address conduct that is similar to conduct addressed by the Act. The Commissioner of Competition may provide assistance to a foreign organisation

under section 74.012 for reviewable matters and under section 52.02 for matters that are prohibited. These provisions allow for instance, the CBC to obtain court ordered records on behalf of a foreign law enforcement agency, without the CBC conducting its own investigation.

Section 74.012 is as follows.

> (1) The Commissioner may, for the purpose of assisting an investigation or proceeding in respect of the laws of a foreign state, an international organization of states or an international organization established by the governments of states that address conduct that is substantially similar to conduct that is reviewable under section 74.01, 74.011, 74.02, 74.04, 74.05 or 74.06,
>
> (a) conduct any investigation that the Commissioner considers necessary to collect relevant information, using any powers that the Commissioner may use under this Act to investigate conduct that is reviewable under any of those sections; and
>
> (b) disclose the information to the government of the foreign state or to the international organization, or to any institution of any such government or organization responsible for conducting investigations or initiating proceedings in respect of the laws in respect of which the assistance is being provided, if the government, organization or institution declares in writing that
>
> (i) the use of the information will be restricted to purposes relevant to the investigation or proceeding, and
>
> (ii) the information will be treated in a confidential manner and, except for the purposes mentioned in subparagraph (i), will not be further disclosed without the Commissioner's express consent.
>
> (2) Subsection (1) does not apply if the contravention of the laws of the foreign state has consequences that would be considered penal under Canadian law.
>
> (3) In deciding whether to provide assistance under subsection (1), the Commissioner shall consider whether the government, organization or institution agrees to provide assistance for investigations or proceedings in respect of any of the sections mentioned in subsection (1).

Section 52.02 is as follows.

> (1) The Commissioner may, for the purpose of assisting an investigation or proceeding in respect of the laws of a foreign state, an international organization of states or an international organization established by the governments of states that address conduct that is substantially similar to conduct prohibited under section 52, 52.01, 52.1, 53, 55 or 55.1,
>
> (a) conduct any investigation that the Commissioner considers necessary to collect relevant information, using any powers that the Commissioner may use under this Act or the Criminal Code to investigate an offence under any of those sections; and
>
> (b) disclose the information to the government of the foreign state or to the international organization, or to any institution of any such government or organization responsible for conducting investigations or initiating proceedings in respect of the laws in respect of which the assistance is being provided, if the government, organization or institution declares in writing that
>
> (i) the use of the information will be restricted to purposes relevant to the investigation or proceeding, and
>
> (ii) the information will be treated in a confidential manner and, except for the purposes mentioned in subparagraph (i), will not be further disclosed without the Commissioner's express consent.
>
> (2) In deciding whether to provide assistance under subsection (1), the Commissioner shall consider whether the government, organization or institution agrees to provide assistance for investigations or proceedings in respect of any of the sections mentioned in subsection (1).

European Union

The new CPC Regulation, which entered into force in the EU and EEA on 17 January 2020, has improved the effectiveness and efficiency of the mutual assistance mechanism by setting time limits for information requests and providing that necessary investigation and enforcement measures should be adopted in a timely manner. The Regulation can be activated to enforce intra-EU cross border infringements of 27 bodies of EU consumer protection legislation.

The CPC co-operation mechanisms are applicable to business-to-consumer transactions including legal acts covering unfair commercial practices, e-commerce, unfair contract terms, geo-blocking, portability of audio-visual content, digital contracts and guarantees, package holidays, retail financial services, and passenger rights. Currently the CPC Regulation covers 27 legal acts, which are included in its annex.

Article 11 of the Regulation specifies the procedure for information requests, specifically:

> 1. At the request of an applicant authority, a requested authority shall, without delay, and in any event within 30 days unless otherwise agreed, provide to the applicant authority any relevant information necessary to establish whether an intra-Union infringement has occurred or is occurring, and to bring about the cessation of that infringement.
>
> 2. The requested authority shall undertake the appropriate and necessary investigations or take any other necessary or appropriate measures in order to gather the required information. If necessary, those investigations shall be carried out with the assistance of other public authorities or designated bodies.
>
> 3. On request from the applicant authority, the requested authority may allow officials of the applicant authority to accompany the officials of the requested authority in the course of their investigations.

The Regulation also specifies the procedure for mutual assistance in Article 13, including the information that the applicant authority should provide. The reasons for refusing to provide mutual assistance are described in Article 14. In the event of a disagreement between the applicant authority and the requested authority on whether the assistance should be provided or not, either of the authorities may refer the matter to the European Commission, which shall issue an opinion on the matter without delay. The European Commission supervises the mutual assistance mechanism and can also issue opinion guidance or advice on its own initiative.

Ireland

The Competition and Consumer Protection Act 2014, section 23(1) provides that the Irish CCPC may, with the consent of the relevant minister, enter into arrangements with a foreign competition or consumer body whereby each party to the arrangements may:

a. Furnish to the other party information in its possession if the information is required by that other party for the purpose of performance by it of any of its functions.

b. Provide such other assistance to the other party as will facilitate the performance by that other party of any of its functions.

United States

The Federal Trade Commission Act (as amended by the US SAFE WEB Act) 15 U.S.C. § 46(j) permits the US FTC to use its compulsory process to obtain information to aid a foreign law enforcement agency that is investigating or engaging in enforcement proceedings against possible violations of laws prohibiting fraudulent or deceptive commercial practices, or other practices substantially similar to practices prohibited by any provision of the laws administered by the FTC. The conduct identified in the request need not constitute a violation of US law. The Act provides several criteria, including whether the requesting agency has provided or agreed to provide reciprocal assistance to the FTC; whether the assistance is in the public

interest; and whether the requesting agency's investigation or enforcement proceeding concerns acts or practices that cause or are likely to cause injury to a significant number of persons.

The agency may use its own compulsory process or the mechanisms for international judicial assistance under the United States Code, 28 U.S.C. § 1782, which allows "any interested person" to file directly in a US federal district court to obtain information (including documents, testimony, and electronically stored evidence) located in the district in which the court is located to obtain evidence for use in an international or foreign tribunal. The foreign proceeding that forms the basis for the §1782 application need not be pending or even imminent. Rather, it need only be in "reasonable contemplation"; however, most US courts require that the foreign proceeding (or contemplated foreign proceeding) be adjudicative in nature. The statute does not require that the information be discoverable in the foreign jurisdiction, although it provides protection for materials that would be privileged under foreign law. See *Intel Corp v Advanced Micro Devices, Inc*., 124 S. Ct. 2466 (2004) (upholding order directing Intel to produce documents from a US private antitrust suit for use by ADM in connection with a complaint filed by ADM with the European Commission).

Examples from the competition area

Article 22 of Council Regulation (EC) No 1/2003 provides that the competition authority of an EU member state may in its own territory carry out any inspection or other fact-finding measure under its national law on behalf and for the account of the competition authority of another member state in order to establish whether there has been an infringement of EU competition law. Any exchange and use of the information collected must be carried out in accordance with Article 12, which governs exchange of information.

The new Directive (EU) 2019/1 of 11 December 2018, known as the ECN+ Directive, strengthens the investigatory assistance measures provided pursuant to Article 22. In particular, Article 24 of the ECN+ Directive ensures that competition authorities in EU member states shall be empowered in their own territory to exercise the powers to carry out an inspection or interview on behalf of and for the account of other national competition authorities, and the officials of the requesting competition authorities shall be permitted to attend and actively assist the requested national competition authority in these activities.

Considerations and good practice tips

In addition to serving the public interest, robust domestic enforcement powers promote reciprocal assistance from foreign enforcement authorities, which also provides for efficient use of limited resources.

Some countries may have the legal authority to assist others by expanding the scope of their own existing investigations, but would find it difficult or legally impossible to start a new investigation in order to assist another country. Accordingly, such countries may wish to consider removing such restrictions or putting mitigations in place.

The EU's experience with the old CPC Regulation and the new CPC Regulation has shown that it is extremely important to have a time limit to responding to requests from foreign authorities in the European context. The supervising role of the European Commission on the functioning of the mutual assistance mechanism helps to ensure that such mechanism is used efficiently. The fact that EU consumer legislation is fully harmonised makes it easier for CPC authorities in the EU to assist each other and agree on the legal assessment of the infringements. In practice, CPC authorities co-operate by using a common legal "dictionary" from the text of the EU Directives and Regulations and refer to this text when they resolve bilateral demands or address multinational traders.

Guiding principle 3: Application of investigatory powers to foreign businesses

> The 2003 Cross-border Fraud Recommendation states that Adherents should provide for "Effective mechanisms to adequately investigate, preserve, obtain and share relevant information and evidence relating to occurrences of fraudulent and deceptive commercial practices." (Part II, A, 2)
>
> The 2016 E-commerce Recommendation provides that Adherents should "Establish and maintain consumer protection enforcement authorities that have the authority and powers to investigate and take action to protect consumers against fraudulent, misleading or unfair commercial practices [and] Work towards enabling their consumer protection enforcement authorities to . . . take action against foreign businesses engaged in fraudulent and deceptive commercial practices against domestic consumers." (Part Two, Para 53 (iii)-(iv)). It also provides that Adherents should "Improve the ability of consumer protection enforcement authorities and other relevant authorities, as appropriate, to co-operate and co-ordinate their investigations and enforcement activities, through notification, information sharing, investigative assistance and joint actions." (Part Three, Para 54 (ii)).

Sources 2003 Cross-Border Fraud Recommendation, Part II, A, 2; 2016 E-commerce Recommendation, Part Two, Para 53(iii)-(iv), and Part Three, Para 54(ii); also relevant to UN Guidelines for Consumer Protection, paragraphs V.A. 15, V.I.; 79 (a), 88, 90.

Rationale

Given the spread of global e-commerce and leisure travel, it is common for consumers to contract with businesses outside their own jurisdiction. As cross-border private legal action can be extremely difficult in practice for consumers to pursue, and foreign enforcement authority resources or legal systems may not allow for effective enforcement action on behalf of non-citizens, it may be necessary for consumer protection enforcement agencies to obtain information from businesses and persons outside their own borders when their own consumers have been affected.

As the complexity of international law, applicable law and disputes over jurisdictions are likely to make such interactions challenging in practice; the crucial concept here is for domestic law to actively enable consumer protection enforcement agencies to take such action, rather than prohibiting or inhibiting agencies from investigating cross-border unlawful conduct. The existence of such authority, however, would not require a foreign consumer protection enforcement agency to recognise and enforce an information request from a foreign agency nor would it preclude the foreign agency from declining to provide assistance or to impose conditions on such assistance based on genuine concerns such as data protection and privacy, confidentiality, due process, international law, and mutual legal assistance. Nonetheless, legislators could consider whether statutes that provide for blanket prohibitions against companies or courts complying with foreign information requests or other investigatory actions could be removed or modified. Blanket provisions that make it impossible or difficult in practice for foreign consumer protection enforcement agencies to take appropriate action, could also be carefully examined and removed, or modified as part of a legislative or administrative review of such provisions, in accord with each country's practice (as discussed under Guiding principle 5). Consumer protection agencies could also assist in mitigating the effects of such blanket provisions by using their own powers to assist foreign counterparts when such assistance would be lawful.

An explicit power for national courts, authorities and legal entities to co-operate with reasonable and necessary actions by foreign consumer protection enforcement agencies could provide an ideal outcome, though it is appreciated this may need to be balanced by appropriate safeguards such as around individual data protection and privacy and genuinely commercially sensitive materials held by corporate and other trading entities as well as international law concerns.

Detail of the powers

Clear power

The domestic legislation that confers power on the consumer protection enforcement agency to require production of information could be drafted without geographical restrictions; however, in enforcing such legislation, consumer protection enforcement agencies could be required to consider relevant principles of international law.

Such legislation could clearly indicate that it applies to any person who directs their business activities towards consumers in the consumer protection enforcement agency's state, and that it applies to protect foreign consumers from businesses operating from the consumer protection enforcement agency's state.

It could further require the production of any relevant information that is accessible to the recipient of the information request or demand, e.g., it is within the custody or control of the recipient, even if that information is physically located outside the recipient's jurisdiction.

Enforceability

An information request issued by a consumer protection enforcement agency in another state could be directly enforceable in the recipient's state in appropriate circumstances. However, given the divergences in substantive law and enforcement practice which exist, it is likely that this might require a binding international agreement. Further, some safeguards are likely to be necessary in the context of such enforcement:

a. There could be a requirement that the substantive infringement under investigation is substantially similar to an infringement in the business's state.

b. In addition, there could be a requirement that the type of information being sought is one which could be required to be produced by a consumer protection enforcement agency in the recipient's state -for example in some states there are restrictions on the production of personally sensitive, legally privileged, or confidential business information. In that case, the enabling legislation could also recognise legitimate exceptions.

c. The local consumer protection enforcement agency could carry out their own assessment of whether the information sought is necessary, whether the quantity of information being sought is proportionate, and whether the request otherwise appears to be in the public interest as well as other discretionary decisional factors.

Statutory example

United States

The Federal Trade Commission Act allows the US FTC to serve a CID or enforcement petition upon individuals and entities located outside the United States in such manner as the US Federal Rules of Civil Procedure, which govern judicial procedures in US federal courts, prescribe for service of a complaint or summons in a foreign nation (FTC Act, Sec. 57b-1(c)(7)(B)). Although the FTC uses this provision in appropriate circumstances, in practice, the agency often seeks information from US entities in possession, custody, or control of relevant information from related foreign entities, relies on voluntary evidence-gathering, and engages in co-operation with foreign counterparts to avoid any conflicts with relevant principles of international law.

Area II: Enforcement outcomes

Guiding principle 4: Enforcement powers to protect domestic consumers from foreign businesses

> The 2003 Cross-border Fraud Recommendation states that Adherents should "work toward enabling their consumer protection enforcement agencies to take action against foreign businesses engaged in fraudulent and deceptive commercial practices against their own consumers." (Part V, C)
>
> The 2016 E-commerce Recommendation provides that Adherents should work towards enabling their consumer protection enforcement agencies "to take action against foreign businesses engaged in fraudulent and deceptive commercial practices against domestic consumers" (Part Two, Para 53 (iv)).
>
> In addition, the 2007 Dispute Resolution and Redress Recommendation provides that Adherents should work to improve cross-border redress mechanisms including "[d]eveloping multi-lateral and bi-lateral arrangements to improve international judicial co-operation in the recovery of foreign assets and the enforcement of judgments in appropriate cross-border cases."

Sources: 2003 Cross-Border Fraud Recommendation, Part V, C; 2016 E-commerce Recommendation Part Two, Para 53 (iv); 2007 Dispute Resolution and Redress Recommendation; also relevant to UN Guidelines for Consumer Protection, Paragraphs V.A. 15, V.I.; 79 (a), 88, 90.

Rationale

Where a business directs their commercial activities towards consumers in another state, the consumers there should ideally enjoy the same core protections against fraudulent and deceptive commercial practices, no matter the location from which the business with whom they are dealing is based.

Further, consumer protection enforcement agencies in the consumer's jurisdiction should ideally have the established power to pursue the same core remedies against foreign businesses as they would be able to seek against businesses in their jurisdiction. Guiding principle 6 sets out the remedies to which all consumer protection enforcement agencies should have access.

The legal authority for a consumer protection enforcement agency to take action against a foreign business or person in its own jurisdiction may be sufficient – in particular where there is a means of enforcing against the business, such as assets or business connections in the jurisdiction. Ideally, however, there should be some mechanism that permits an appropriate enforcement remedy made in one jurisdiction to be recognised and enforced in the other jurisdiction, e.g. through the administrative or judicial processes of the foreign jurisdiction, subject to appropriate safeguards based on as data protection and privacy, confidentiality, due process, international law, and mutual legal assistance and any discretionary limits imposed.

Such safeguards could include a requirement that the substantive infringement be substantially similar to a law in the business's domicile. Because this is a complex area that has been the subject of prolonged discussions in the context of various international conventions, it is not set out in further detail in this paper.

Detail of the powers

Scope of applicable law

As with Guiding principle 3, the core protections enforced by the consumer state's consumer protection agency should ideally apply to businesses whose conduct causes consumer harm in that state, regardless of the business's location, as well as to businesses in the jurisdiction causing harm to consumers elsewhere.

Scope of jurisdiction of courts

To the extent reasonable given the general jurisdictional principles of a given court system and principles of international law, consumer protection agencies from that jurisdiction should ideally be able to pursue domestic administrative or judicial remedies against foreign businesses that target and harm the jurisdiction's consumers to the same extent they can use such remedies against domestic businesses. When applicable, they should ideally also have at least discretionary authority in appropriate cases to pursue remedies for foreign as well as domestic consumers as to conduct by domestic businesses (as discussed under Guiding principle 5).

Scope of enforcement power

Countries might consider the extent to which the consumer protection agency in a consumer's state should have the power to investigate businesses, no matter where they are domiciled, where either harmful conduct or foreseeable consumer harm occurs within the consumer's state. An additional consideration is whether a consumer protection enforcement agency should also have at least the discretionary authority to help foreign counterparts to investigate such conduct, when relevant evidence is available in that agency's jurisdiction (as discussed under Guiding principle 2).

Examples

I. Case examples

Yellow Pages business directory scam

A European–based directory scam that defrauded small businesses and non-profit organisations out of millions of dollars by deceiving them into ordering and then paying for unwanted listings in online business directories targeted consumers in Australia, Canada, the United States, and other jurisdictions. The individuals behind the scheme were based in Spain, used Dutch and UK corporations, and operated a range of websites and accommodation addresses in multiple jurisdictions. As a result of multi-jurisdictional intelligence sharing that led to the quick identification of emerging issues, global deterrence, and effective enforcement outcomes, enforcers in several jurisdictions took action against foreign traders to protect consumers within their jurisdiction.

The ACCC brought the first court proceeding against two of the overseas companies, Yellow Page Marketing BV (Netherlands) and Yellow Publishing Limited (UK), in 2010. In 2011, the US FTC and the CBC filed parallel court actions against various Yellow Pages defendants, both within and outside their borders. After learning that certain organisations, including Factoring International AG, a Swiss company, contacted consumers to collect on Yellow Page Marketing invoices after the courts had enjoined collection of such invoices, the agencies also co-operated with the Swiss State Secretariat for Economic Affairs, which sent a warning letter to the Swiss company. The agencies also worked with the UK National Fraud Intelligence Bureau, which took action to eliminate the harm caused by deceptive use of virtual offices in the United Kingdom.

The jurisdictions involved relied on statutory authority permitting them to sue foreign traders. The FTC relied on the provisions of the US SAFE WEB Act that allow the FTC to bring enforcement actions when it is "reasonably foreseeable" that a foreign defendant's conduct will cause harm to consumers In the United

States. The FTC also relied on the information sharing provisions of the SAFE WEB Act share information it had obtained through compulsory process with the CBC.

In 2011, the ACCC's action resulted, among other things, in penalties of AUD 2.7 million and injunctions restraining the foreign entities from specific registering domain names including the words "yellow page/s" in combination with ".au" or the name of a city, state or other location in Australia. The CBC's action resulted in CAD 9 million (Canadian dollars) in penalties and other injunctive relief. The FTC obtained a court order providing for USD 10.2 million in monetary consumer redress, permanently banning the defendants from marketing Internet directories and listings in the future, and prohibiting defendants from collecting payments or disclosing or benefitting from customers. The FTC intercepted 800 checks totalling USD 460 000 from mail sent by consumers to Yellow Pages' US address. The FTC destroyed the checks to protect consumers' information. Although the coordinated court actions disrupted the scheme and raised consumer awareness of fraudulent business directory schemes, the agencies were not able to recover assets from offshore jurisdictions to satisfy the full amount of fines and monetary redress ordered.

Australia

In 2014, the ACCC alleged that Valve, an online game developer and distributor based in the United States, had unlawfully excluded statutory guarantees of acceptable quality, and made representations that sought to prevent consumers seeking remedies for failure to comply with the guarantees. Valve's representations that refunds would not be made in any circumstances were alleged to be false and misleading as the company was legally obligated to provide refunds to Australian consumers in some circumstances. Valve argued that the Australian Consumer Law (ACL) did not apply to it as the Subscriber Agreement was governed by Washington State law in the United States. However, the Full Federal Court of Australia held the ACL applied to Valve despite its lack of physical presence in the Australia, as Valve was considered to be carrying on a business in Australia within the meaning of section 5(1)(g) of the Competition and Consumer Act. This was on the basis of a number of reasons, including that Valve had many customers in Australia and owned servers in Australia upon which content was "deposited" when requested by its Australian customers. The fact that the contractual relationship between Valve and its customers was governed by Washington State law provided no protection. Accordingly, in 2017 the Court affirmed an AUD 3 million penalty levied against Valve for contraventions of the ACL.

Peru

The Technical Secretariat of the Commission on Unfair Competition of the National Institute for the Defense of Free Competition and the Protection of Intellectual Property (Indecopi) started a preliminary investigation against Cap Technologies S.A.S. (known in Peru as "Picap") for advertising their mobile application named "Picap", which allegedly violated the rules of the Legislative Decree 1044 (Unfair Competition Law). Since Cap Technologies S.A.S is based in Colombia and given that it was being investigated in Colombia as well, the Technical Secretariat established contact with the Superintendence of Industry and Commerce of Colombia (SIC). In January 2020, coordination with the SIC began, through phone calls. It was agreed to physically send relevant documents to the SIC, in order for them to transfer the documents to the investigated corporation. On March 4 2020, an ex officio procedure against Cap Technologies S.A.S. was initiated and the documents were sent to the SIC for their subsequent notification. Thereafter, through e-mail, the SIC sent the Cap Technologies S.A.S. Chamber of Commerce a Single Business Registration document and recommended to electronically notify the procedure initiated ex officio to the e-mail address established in that document. This procedure was completed in the first instance on February 23, 2021 and the Commission on Unfair Competition decided Cap Technologies S.A.S had violated the Unfair Competition Law and fined it with 20 UIT (Peruvian tax units).

United Kingdom

The UK Office of Fair Trading (OFT) received complaints in 2008 from UK consumers regarding a Dutch company Best Sales B.V. that sent unsolicited mail to UK consumers giving them the impression that they

had won a prize. The mail stated that in order to receive a more valuable prize or to receive this prize more rapidly, the consumers needed to order articles from the catalogue. The OFT brought an action against the company before the Dutch courts. In a ruling on 9 July 2008, the Dutch courts considered the advertising misleading and ordered the company to stop sending the advertising.

II. Statutory examples

Australia

The Competition and Consumer Act 2010, section 5(1), extends the application of the Australian Consumer Law to conduct outside Australia by bodies corporate incorporated or carrying on business within Australia. As a result, even if a business does not have a physical presence in Australia, that business can still be subject to the Australian Consumer Law to the extent that the business is considered to be "carrying on a business" in Australia. This was clarified by the Full Federal Court of Australia in the ACCC's case against Valve, an online game distributor located in the United States (see case example above).

Furthermore, the Competition and Consumer Act 2010, section 5(1A), extends the application of the Australian Consumer Law to conduct outside Australia by New Zealand and New Zealand Crown corporations bodies corporate carrying on business within New Zealand.

European Union

The Injunctions Directive (Directive 2009/22/EC) harmonises the relevant rules across EU & EEA member states to ensure that injunctions are effective in a cross-border dimension. The Directive gives qualified entities (consumer organisations or independent public bodies) with a legitimate interest in protecting the collective interests of consumers, the power to pursue enforcement actions designated to bring an end to the infringement directly in the courts or administrative authority of another EU/EEA member state. The infringements that may be considered as harming the collective interests of consumers include those relating to directives on consumer credit, package travel, unfair terms in contracts concluded with consumers, distance contracts and unfair commercial practices.

Under the Directive, each EU and EEA member state shall take the measures necessary to ensure that, in the event of an infringement originating in that member state, a qualified entity from another member state where the interests protected by that qualified entity are affected by the infringement, may apply for an injunctive order to its competent court or administrative authority. Only qualified entities designated by the EU & EEA member states and enumerated in the publicly available EU list can pursue such cross-border action. The possibility of bringing a cross-border injunction action is also subject to the EU private international law rules on jurisdiction and applicable law. This mechanism would allow a consumer protection enforcement agency – if designated by an EU & EEA member state as qualified entity and placed at the EU list – to take enforcement actions against a business in its home state.

The Directive (EU) 2020/1828 on Representative Actions, to be applied in the EU from 25 June 2023, will provide for even more opportunities for the cross-border enforcement of consumer rights through the representative actions for injunctive and redress measures. According to this Directive, each qualified entity (an organisation or public body) designated by an EU member state under the Directive, could represent consumers from several or all EU member states in a specific action, subject to EU private international law rules (Art. 2(1) and (3), Art. 3(6-7), Art. 6 (1 and 3) and Recitals 23 and 31). In addition, the Directive offers the opportunity for the qualified entities designated in different EU member states of acting jointly within a single action in front of a single competent forum within the EU (Art. 6(2 and 3)). The representation of different organisations from different EU member states could also take place in case of an action brought by a European "chapeau" organisation, if designated as qualified entity in an EU member state (Art. 4(2)).

United Kingdom

The Enterprise Act 2002, Part 8, section 210(5), confers on UK consumer protection enforcement agencies the power to take enforcement actions for the protection of consumers from infringements, irrespective of where the trader is based. For the purposes of 'domestic infringements', section 210(5) states that "it is immaterial whether a person supplying goods or services has a place of business in the United Kingdom." This indicates that, in principle, actions can be taken against overseas businesses with no geographical restrictions so long as the infringement has taken place domestically.

United States

The Federal Trade Commission Act, amended by the US SAFE WEB Act, section 5(a)4(A), 15 U.S.C. 45 § (a)4(A), provides the US FTC with the ability to take enforcement action involving foreign commerce when there are unfair or deceptive acts or practices that (i) cause or are likely to cause reasonably foreseeable injury within the United States; or (ii) involve material conduct occurring within the United States. § 5(a)4(B) furthermore provides that all remedies generally available to the FTC with respect to unfair and deceptive acts or practices shall be available for acts and practices (i) and (ii), including restitution to domestic or foreign victims.

Considerations and good practice tips

Some countries may have explicit legal limitations on taking action when the trader is not based in their country or does not have a place of business/establishment, for example. Where possible, these countries may consider ways to avoid such explicit restrictions.

Guiding principle 5: Enforcement powers to protect foreign consumers from domestic businesses

> The 2003 Cross-border Fraud Recommendation states that Adherents should "work toward enabling their consumer protection enforcement agencies to take action against domestic businesses engaged in fraudulent and deceptive commercial practices against foreign consumers." (Part V, B)
>
> The 2016 E-commerce Recommendation provides that Adherents should "Work towards enabling their consumer protection enforcement authorities to take action against domestic businesses engaged in fraudulent and deceptive commercial practices against foreign consumers" (Part Two, Para 53 (iv)).

Sources: 2003 Cross-Border Fraud Recommendation, Part V, B; 2016 E-commerce Recommendation, Part Two, Para 53 (iv); also relevant to UN Guidelines for Consumer Protection, Paragraphs V.A. 15, V.I.; 79 (a), 88, 90.

Rationale

Providing consumer protection authorities with the legal authority to investigate and sue domestic businesses that harm foreign consumers (in addition to domestic consumers or, in appropriate cases, only foreign consumers) can help ensure that jurisdictions do not become havens for businesses that operate fraudulent schemes or companies that engage in other deceitful or harmful commercial practices. It can prevent unscrupulous businesses from establishing a base in one jurisdiction and exporting frauds and other harmful commercial practices to another jurisdiction without fear of regulatory scrutiny or law enforcement action. It also ensures that agencies have the authority to carry out enforcement co-operation commitments under bilateral or multilateral agreements.

The consumer agency where the business is located may be in the best position legally and logistically to conduct the investigation. Indeed, given limits on international recognition of penalties, it may also be best positioned to pursue remedies.

The authority to investigate and sue businesses for harms to foreign consumers, and in certain cases, to provide them with remedies such as monetary restitution, can also help to build a robust culture of reciprocity among consumer protection enforcement agencies. It can provide evidence to government ministries and legislators of the benefits of international consumer protection enforcement co-operation.

Examples

I. Case examples

European Union

In 2020, under the CPC Regulation, EU and EEA authorities submitted 113 enforcement requests aiming at asking an authority in another EU/EEA member state to take enforcement measures against a trader established in their jurisdiction, but believed to engage in fraudulent and misleading practices in another EU/EEA member state. 23 requests were successfully completed, the remaining requests were still being handled at the end of 2020.

As an example, the consumer protection authority in another EU member state requested the Swedish Consumer Agency take actions against a Swedish trader that targeted and harmed consumers in the requesting authority's member state. The Swedish Consumer Agency took actions by contacting the trader, which resulted in the trader making the requested changes on its website to stop the infringement. The issue was solved, and the case closed.

United States

The US FTC filed an enforcement action against a US-based online electronics retailer and related defendants that tricked UK consumers into believing it was based in the United Kingdom by using foreign websites ending in ".co.uk." The defendants targeted UK consumers who complained that they had been charged unexpected import duties, were provided with invalid warranties, and were told they would be charged draconian cancellation and refund fees if they attempted to send the merchandise back. The FTC entered into a settlement agreement with the defendants that prohibited them from misrepresenting, among other things, the location, quality, quantity, characteristics, and model numbers of products they sell; their policies regarding cancellation, exchange, or return; the existence of product warranties; and the total cost of the products sold. It also banned the company from charging consumers for goods until they are in hand and ready to be shipped.

The FTC has an online portal showing monetary redress provided to both domestic and foreign consumers. For the cases currently listed (involving some disbursement since July 2018), the FTC sent international checks to approximately USD 5.7 million to nearly 36 000 non-US consumers in 85 countries as redress in 86 cases. (This number excludes redress paid via electronic payments for which there is no geographic location information).

Example from the securities area

In 2016 the US Securities Exchange Commission (SEC) brought an action against a US-based individual, Charles Scoville and his company, Traffic Monsoon, an internet website exchange that offered its members USD 50 "Adpacks," to help make their websites appear more popular than they actually are on search engines such as Google. Each "Adpack" included 1 000 website visits and 20 clicks on advertisement banners, and gave purchasers a right to share in Traffic Monsoon's profits up to USD 55 per "Adpack." Traffic Monsoon also encouraged members to recruit other members, and receive a 10% commission on every service purchased by the recruited member.

In its enforcement action, the SEC alleged that Traffic Monsoon was not a bona fide website traffic exchange but instead was operating as a Ponzi scheme with more than 99% of its revenue coming from other participants, not products and services. Notably nearly 90% of "Adpack" purchasers were located outside the United States in countries like Bangladesh, Morocco, and Venezuela. The defendants challenged the application of the SEC's anti-fraud provisions to a case involving mostly foreign victims. The lower court ruled that the SEC could challenge such conduct even though the vast majority of purchasers were abroad. On appeal, the appellate court held the substantive antifraud provisions of the SEC covered Traffic Monsoon's conduct due to the significant conduct in the United States, including the sale and advertising of "Adpacks." (SEC v. Traffic Monsoon, LLC, 245 F. Supp. 3d 1275 (D. Utah 2017), aff'd, SEC v. Scoville, et al., No. 17-4059, 2019 WL 302867, *1 (10th Cir., Jan. 24, 2019)). On 5 August 2020, the United States obtained a criminal indictment against the defendants, charging them with wire fraud under 18 U.S.C. § 1343 and tax fraud under 26 U.S.C. § 7206. On 5 January 2021, the court ordered Scoville to pay nearly USD 5 million, including USD 2.5 million in redress to the victims of the scheme.

II. Statutory examples

European Union

Within the EU, the CPC Regulation creates an obligation on EU member states to co-operate in bringing to an end any cross-border infringements of laws that protect consumers' interests. Within the EU, infringements of consumer protection legislation should be dealt with by consumer protection enforcement agencies in the jurisdiction where the business responsible for the practice is situated, and in the same way as an infringement affecting domestic consumers would have been dealt with, in order to avoid discrimination between domestic and intra-EU transactions (CPC Regulation, Article 11: "Competent authorities shall fulfil their obligations under this Regulation as though acting on behalf of consumers in their own country").

As detailed in Article 12 of the CPC Regulation, the national authority in the jurisdiction where the business responsible for the practice is situated ("the requested authority") shall:

- Take all necessary and proportionate enforcement measures to bring about the cessation or prohibition of the infringement.
- Determine the appropriate enforcement measures needed to bring about the cessation or prohibition of the infringement.
- Take such measures without delay and not later than 6 months after receiving the request, unless it provides specific reasons for extending that period.
- Where appropriate, impose penalties, such as fines or periodic penalty payments, on the trader responsible for infringement. The requested authority may also receive from the trader, on the trader's initiative, additional remedial commitments for the benefit of consumers that have been affected by the alleged infringement, or, where appropriate, may seek to obtain commitments from the trader to offer adequate remedies to consumers that have been affected by that infringement.
- Regularly inform the applicant authority about the steps and measures taken and the steps and measures that it intends to take and keep informed all member states through the electronic system whether interim measures have been imposed; whether the infringement has ceased; which measures have been adopted, and whether those measures have been implemented; and the extent to which consumers affected by the alleged infringement have been offered remedial commitment.

As this is the case for information requests, the Regulation also specifies the procedure for mutual assistance and enforcement requests in Article 13, including the information that the applicant authority

should provide. The reasons to refuse to provide mutual assistance are described in Article 14. These reasons are:

> (a) criminal investigations or judicial proceedings have already been initiated, or there is a judgment, a court settlement or a judicial order in respect of the same intra-Union infringement and against the same trader before the judicial authorities in the Member State of the requested authority;
>
> (b) the exercise of the necessary enforcement powers has already been initiated, or an administrative decision has already been adopted in respect of the same intra-Union infringement and against the same trader in the Member State of the requested authority in order to bring about the swift and effective cessation or prohibition of the intra-Union infringement;
>
> (c) following an appropriate investigation, the requested authority concludes that no intra-Union infringement has occurred;
>
> (d) the requested authority concludes that the applicant authority has not provided the information that is necessary
>
> (e) the requested authority has accepted commitments proposed by the trader to cease the intra-Union infringement within a set time limit and that time limit has not yet passed.

However, the requested authority shall comply with the request for enforcement measures under Article 12 if the trader fails to implement accepted commitments within the time limit referred. In the event of a disagreement between the applicant authority and the requested authority on whether the assistance should be provided or not, either of the authorities may refer the matter to the European Commission, which shall issue an opinion on the matter without delay. The European Commission supervises the mutual assistance mechanism and can also issue opinion guidance or advice on its own initiative.

The Representative Actions Directive to be applied across the EU from 25 June 2023 provides for the possibility for a qualified entity (an organisation or public body) designated by an EU member state under the Directive to bring representative actions for injunctive and redress measures for the protection of the collective interests of consumers from other EU member states, subject to certain conditions and EU private international law rules (Art. 2(1) and (3), Art. 3(6-7), Art. 6(3) and Recitals 23 and 31).

United Kingdom

Enterprise Act 2002, Part 8, section 210, subsections (3) and (4) define the consumer as an individual that satisfies two conditions:

> (3) The first condition is that:
>
> (a) goods are or are sought to be supplied to the individual (whether by way of sale or otherwise) in the course of a business carried on by the person supplying or seeking to supply them, or
>
> (b) services are or are sought to be supplied to the individual in the course of a business carried on by the person supplying or seeking to supply them.
>
> (4)The second condition is that:
>
> (a)the individual receives or seeks to receive the goods or services otherwise than in the course of a business carried on by him, or
>
> (b) the individual receives or seeks to receive the goods or services with a view to carrying on a business but not in the course of a business carried on by him.

In this section the legislator did not specify where the consumer must be in order to be protected. This is addressed in section 211, in the definition of 'domestic infringement':

> 211 Domestic infringements

> (1) In this Part a domestic infringement is an act or omission which—
>
> (a) is done or made by a person in the course of a business,
>
> (b) falls within subsection (2), and
>
> (c) harms the collective interests of consumers
>
> (1A) But an act or omission which satisfies the conditions in subsection (1) is a domestic infringement only if at least one of the following is satisfied—
>
> (a) the person supplying (or seeking to supply) goods or services has a place of business in the United Kingdom, or
>
> (b) the goods or services are supplied (or sought to be supplied) to or for a person in the United Kingdom (see section 232)

Section 211(1)(c) previously specified that there should be harm to the collective interests of consumers "in the United Kingdom" This was removed and replaced by the requirement in s.211(1A), which requires that either the business or the consumer is in the United Kingdom. As a result, where a business based in the United Kingdom deals with consumers elsewhere, it is obliged to comply with UK law, or face the risk of enforcement. Likewise, the courts have the clear power to order non-UK businesses to comply with UK law where they are dealing with UK consumers.

United States

The Federal Trade Commission Act, amended by US SAFE WEB Act, section 5(a)4(A), 15 U.S.C. 45 § (a)4(A), provides the US FTC with the ability to take enforcement action involving foreign commerce when there are unfair or deceptive acts or practices that (i) cause or are likely to cause reasonably foreseeable injury within the United States; or (ii) involve material conduct occurring within the United States. Section 5(a)4(B), 15 U.S.C. 45 § (a)4(B), furthermore provides that all remedies generally available to the FTC with respect to unfair and deceptive acts or practices shall be available for acts and practices (i) and (ii), including restitution to domestic or foreign victims.

Example from the securities area

The US Securities Exchange Act, amended by the Dodd-Frank Act, § 929P(b), 15 U.S.C. § 78aa, provides US federal district courts with jurisdiction over proceedings brought or instituted by the SEC for (1) conduct within the United States that constitutes significant steps in furtherance of [a securities law] violation, even if the securities transaction occurs outside the United States and involves only foreign investors; or (2) conduct occurring outside the United States that has a foreseeable substantial effect within the United States.

Considerations and good practice tips

Consumer protection enforcement agencies may face questions or concerns about their use of resources if they bring an action that primarily or exclusively benefits foreign consumers. Therefore, agencies, in determining which investigations and cases to pursue, may wish to strategically focus on cases that also involve harm to domestic consumers as well as widespread or serious harms to foreign consumers.

The differences of legal systems, in particular if consumer protection authorities can exercise some enforcement powers directly or if they need to have recourse to court authorisation or involvement of other authorities, and the complexity of some enforcement requests, can result in substantial delays to respond to the mutual assistance requests. Therefore, there is a need for clear deadlines (e.g. up to six months in the EU CPC Regulation) but also flexibility to extend these deadlines when duly justified. The reasons to refuse mutual enforcement assistance should be also clearly stated but in case the requested authority is refusing assistance, it should discuss this refusal with the applicant authority.

Guiding principle 6: Minimum enforcement outcomes

The 2003 Cross-border Fraud Recommendation states that Adherents should provide for "Effective mechanisms to adequately investigate, preserve, obtain and share relevant information and evidence relating to occurrences of fraudulent and deceptive commercial practices" (Part II, A, 2) and "Effective mechanisms to stop businesses and individuals engaged in fraudulent and deceptive commercial practices" (Part II, A, 3). It further states that consumer protection enforcement agencies "whose territories are affected by fraudulent and deceptive commercial practices against consumers should have appropriate authority to investigate and take action within their own territory." (Part V, A)

The 2016 E-commerce Recommendation provides that Adherents should "Establish and maintain consumer protection enforcement authorities that have the authority and powers to investigate and take action to protect consumers against fraudulent, misleading or unfair commercial practices and the resources and technical expertise to exercise their powers effectively" (Part Two, Para 53 (iii). It also provides that Adherents should "Improve the ability of consumer protection enforcement authorities and other relevant authorities, as appropriate, to co-operate and co-ordinate their investigations and enforcement activities, through notification, information sharing, investigative assistance and joint actions" (Part Three, Para 54 (ii)).

Sources: 2003 Cross-Border Fraud Recommendation, Part II, A, 2, 3, Part V, A; 2016 E-commerce Recommendation Part Two, Para 53 (iii), Part Three, Para 54 (ii); also relevant to UN Guidelines for Consumer Protection, Paragraphs V.A. 15, 37-41; V.I.;

Rationale

In tackling harm to consumers, it is important that consumer protection enforcement agencies can achieve effective outcomes against the business under investigation, in particular given the development of new technologies – and bring justice for consumers who have been harmed and create a reasonable level of deterrence to encourage other businesses to stay within the limits of the law. Consumer protection enforcement agencies should also be able to achieve these outcomes reasonably efficiently, given that public resources are at stake, and any delay in resolution is likely to lead to continued harm to consumers.

Effective enforcement requires all consumer protection enforcement agencies in jurisdictions where businesses base themselves to have a reasonably consistent set of core powers; otherwise there is a real likelihood that cross border harm will remain unresolved. At its worst, inconsistency in enforcement power can encourage bad actors deliberately to choose to base themselves in places where they are less likely to be held to account.

Detail of the powers

Permanent injunctive orders

The core remedy in tackling consumer harm is ensuring businesses can be stopped or prevented from engaging in illegal conduct in the future. This allows consumer protection enforcement agencies appropriately to shape market conduct to achieve a level playing field between businesses and ensure consumers are protected.

A future looking injunctive power should enable consumer protection enforcement agencies to prevent likely harmful conduct from taking place, where there are good reasons to believe the business is about to embark on illegal conduct (for example where an individual involved in a closed illegal business is setting up a new business with a similar business model); it should also permit consumer protection enforcement agencies to take action against conduct (such as misleading marketing material or unfair terms) which the evidence shows is likely to occur but has not been deployed yet.

The power should not be restricted to prohibiting illegal conduct, but should permit an order to require the business to take positive steps, including for example requiring a specific disclosure to be made to prevent misleading advertising, or requiring the business to give refunds as required in law or under contract.

Where appropriate, an order also should be capable of requiring the business to take steps to put in place measures that are not in themselves general legal requirements, but which are likely to facilitate compliance in particular cases. For example, where the harm is caused by the behaviour of individual sales staff, it would be appropriate for an order to require the business to give them better training, and perhaps to record their interactions with consumers so that allegations of misleading or aggressive selling could be investigated and remedied (even though these requirements are not laid down in a specific law).

In order to bring cases to an efficient conclusion, consumer protection enforcement agencies should be able to accept binding commitments by a business to change in lieu of a court order. However, it is important that such commitments are themselves enforceable in a similar way to a court order in order to incentivise the business to comply with the promises it has given.

Temporary or preliminary injunctive orders

The process to obtain a final order may be time consuming, and with appeals may take several years to reach a conclusion. In the meantime, if the business is able to continue with the conduct, consumers are likely to continue to suffer harm, and other businesses suffer a competitive disadvantage. It is therefore important that, where appropriate, it is possible to require the business to stop engaging in the impugned conduct pending final resolution of the matter.

Temporary relief may also be appropriate where the conduct should be prohibited immediately (for example the conduct is ongoing), and where it is more likely than not that the decision maker would grant a final order prohibiting the conduct.

An interim order should be capable of requiring the business or a third party to take steps to prevent the business from evading justice, such as freezing of the business's assets (for example where there is likely to be a case for giving redress to consumers) or preserving evidence to prevent the destruction of such evidence.

Such orders should be capable of being obtained without notice to the business where necessary (for example where the business would be likely to dissipate assets if put on notice).

Financial recovery

An enforcement system which relies solely on injunctive orders may be of more limited effectiveness because it may incentivise businesses to break the law for as long as they can, and only alter their behaviour when made to stop. Some form of financial recovery, such as fines and consumer redress, is therefore an important part of an enforcement system to incentivise compliance. The practical responsibility for obtaining and distributing financial compensation can be vested with the consumer protection enforcement agency or with another governmental body or private organisation, such as a consumer organisation.

Statutory penalties or fines

Fines, in order to be effective, should be set at a level that is dissuasive. In the most serious cases criminal sanctions may be appropriate as well, in particular where individual directors of businesses are culpable and have deliberately allowed their business to break the law.

The following types of fine should be considered in building an effective enforcement regime:

a. Punishing non-compliance with the law: where a business has been found to be in breach of the law, the consumer protection enforcement agency should be able to secure a fine to punish non-compliance. This is particularly important where several

businesses have agreed to come into compliance at a fixed time - since the delay by any one of them will create an uneven playing field.

b. Punishing non-compliance with orders: any injunctive system needs to be backed up by credible sanctions, so that businesses do not benefit by incomplete or delayed compliance with the order. In some jurisdictions, this framework is provided by the rules on punishing non-compliance with court orders generally (contempt of court).

c. Punishing non-compliance with promises to change: it is often expedient for a consumer protection enforcement agency to accept a binding commitment from a business to change their conduct. However, if the business is able to depart from these commitments with impunity, this wastes public resources expended in the original investigation, and undermines trust in the enforcement system.

d. Removing unlawfully obtained income: where it is impossible or inappropriate to provide redress to individual consumers, but where the business can be shown to have derived income as a result of harming consumers by their unlawful practices, fairness may demand the disgorgement of ill-gotten gains. This resolves the competitive damage suffered by other businesses which did comply, and acts as a further disincentive for businesses to chance their arm by engaging in illegal conduct in the first place.

Redress for consumers

Where consumers have suffered economic harm as a result of the business's illegal conduct, a consumer protection agency may be well placed to require the business to provide redress. This could include:

a. Return of monetary payments: for example, where the consumer has paid too much for a product as a result of misleading claims, the return of the difference between the price paid and the actual market value; where the consumer has paid money which the business was not contractually entitled to, the return of all of that money.

b. Return of property taken by the business: for example, where the consumer is tricked into handing over property to the business or accepting an unfairly low price as a result of misleading claims.

c. Compensation for loss or damage suffered by the consumer: for example, where the business has caused damage to the consumer's other possessions, or caused them harassment or distress as a result of aggressive selling techniques.

d. Termination of contract: for example, where the consumer has been persuaded by misleading claims to enter into a contract under which they must make payments, they may wish to terminate the contract and so avoid liability for these payments.

Legislators should consider the practicability in their domestic environment of a scheme under which a consumer protection enforcement agency can organise redress to be paid collectively -so that individual consumers do not have each to bring their own claims, and businesses do not face multiple actions. Because of the prevalence of cross border businesses in the modern economy, such schemes should allow payments to be made to consumers who are abroad.

The details of any such collective redress scheme should prevent double recovery by consumers but should not require what amounts to individual litigation of each case of loss. The legislation may also make provision for the business to pay for the collective redress scheme's operation.

Publicity

Enforcement outcomes should be made public. Doing so ensures businesses are held to account and are discouraged from returning to illegal behaviour. Public statements also help to educate consumers and inform the public about the work of the consumer protection enforcement agency. Sometimes a corrective statement by a business is also essential in putting things right.

Legislation should therefore make clear that consumer protection enforcement agencies can:

a. Require statements to be published by businesses to publicise the outcome of enforcement as well as to correct misleading statements.

b. Themselves publish the details of the enforcement action taken against the business and the outcome secured.

Disruption measures

There are many instances of cross-border and internet trade where it is practically impossible or disproportionately difficult to identify a bad actor or bring them to account. Examples include where a business is based in a jurisdiction that has ineffective enforcement laws, or where a business sells on an online interface with false contact details.

In such cases the only means open to the consumer protection enforcement agency to protect consumers from ongoing harm may be to ask a third party to cease providing services to the business that is causing the harm. Examples of such third parties include payment providers whose facilities enable the business to collect payments from the consumers who have been misled and third parties that knowingly assist companies that are illegally harming consumers.

Where the business is engaging in unlawful conduct that harms consumers, legislators should consider in what instances third parties should be held accountable by consumer protection agencies, or should otherwise withdraw services from businesses causing consumer harm, where this is necessary and proportionate.

Recovery of business assets to ensure compliance or secure monetary redress

Ultimately, when a business does not comply with the law or any enforcement outcome or otherwise come into compliance voluntarily, consumer protection enforcement agencies need to have the power to compel compliance. In some circumstances, this may require sanctions, such as taking away a business's ability to operate to comply with a cease-or-desist order, while in other cases this may involve recovery of assets to satisfy an order to provide redress to consumers. Some consumer protection enforcement authorities may have the legal basis to do this at least in the domestic context, as the examples below illustrate. Securing compliance and business assets, however, is usually more difficult in the cross-border context and may require the use of multi-lateral and bi-lateral arrangements on international judicial co-operation on the recovery of foreign assets and the enforcement of judgments.

Examples

I. Case examples

United States

The US FTC has the authority to provide monetary redress to foreign consumers. One example is the FTC's action against the global money transfer company, Western Union, carried out together with the US Department of Justice (DOJ) and the US Postal Inspection Service. The FTC alleged that fraudsters around the world have used Western Union's money transfer system even though the company has long been aware of the problem, and that some Western Union agents were complicit in fraud. The FTC's complaint alleged that Western Union declined to put in place effective anti-fraud policies and procedures and failed to act promptly against problem agents. As a result, in 2017 Western Union agreed to pay USD 586 million in monetary redress and put into place a comprehensive anti-fraud program. To date, approximately USD 300 million in refunds have been provided to 142 000 consumers located in the United States and abroad, who were tricked into using Western Union to pay scammers.

II. Statutory examples

European Union

The EU CPC Regulation requires that the following minimum enforcement powers be granted to national competent authorities (Article 9 of the CPC Regulation):

> (a) the power to adopt interim measures to avoid the risk of serious harm to the collective interests of consumers;
>
> (b) the power to seek to obtain or to accept commitments from the trader responsible for the infringement to cease that infringement;
>
> (c) the power to receive from the trader, on the trader's initiative, additional remedial commitments for the benefit of consumers that have been affected by the alleged infringement or, where appropriate, to seek to obtain commitments from the trader to offer adequate remedies to the consumers that have been affected by that infringement;
>
> (d) where applicable, the power to inform, by appropriate means, consumers that claim that they have suffered harm as a consequence of an infringement about how to seek compensation under national law;
>
> (e) the power to order in writing the cessation of infringements by the trader;
>
> (f) the power to bring about the cessation or the prohibition of infringements;
>
> (g) where no other effective means are available to bring about the cessation or the prohibition of the infringement and in order to avoid the risk of serious harm to the collective interests of consumers:
>
> (i) the power to remove content or to restrict access to an online interface or to order the explicit display of a warning to consumers when they access an online interface;
>
> (ii) the power to order a hosting service provider to remove, disable or restrict access to an online interface; or
>
> (iii) where appropriate, the power to order domain registries or registrars to delete a fully qualified domain name and to allow the competent authority concerned to register it; including by requesting a third party or other public authority to implement such measures;
>
> (h) the power to impose penalties, such as fines or periodic penalty payments, for infringements covered and for the failure to comply with any decision, order, interim measure, trader's commitment or other measure.

As it is the case for investigation powers, enforcement powers foreseen in the CPC Regulation can be exercised by competent authorities directly or by recourse to other competent authorities or other public authorities or by instructing designated bodies, or application to courts competent to grant the necessary decision. The enforcement powers for competent authorities ensure that those authorities can deliver enforcement outcomes when enforcement requests for mutual assistance are addressed to them from authorities from other EU/EEA countries.

In addition, in coordinated actions, which are performed by several competent authorities from different EU countries in the framework of the EU CPC Regulation, authorities have the power to receive from the trader remedial commitments for the benefit of consumers that have been affected by that infringement or to invite the trader to propose such commitments.

Moreover, the Better Enforcement and Modernisation Directive (EU) 2019/2161 has improved enforcement outcomes of coordinated actions under the CPC Regulation. The Directive foresees that where, as a result of the coordinated action under the CPC Regulation, a single competent authority within the meaning of

that Regulation imposes a fine on the trader responsible for the widespread infringement or the widespread infringement with an EU dimension, it should be able to impose a maximum fine at a level that is at least 4 per cent of the trader's annual turnover in all EU member states concerned by the coordinated enforcement action.

The Injunctions Directive 2009/22/EC requires EU & EEA member states to put in place injunction actions aiming at:

- Injunction orders to stop or prohibit infringements of EU & EEA relevant law harming the collective interests of consumers.
- Measures, such as the publication of the injunctions orders and corrective statements (as a deterrent to traders who fear for their reputation).
- Fines in situations where non-compliance persists despite there being an injunctions order, either as a fixed amount or an amount for each day's non-compliance or any other amount (but only in so far as the legal system of the member state permits this).

The Injunctions Directive has been updated and modernised by the Representative Actions Directive (EU) 2020/1828 adding the possibility of redress measures to the types of proceedings already provided by Directive 2009/22/EC. A redress measure shall require a trader to provide consumers concerned with remedies such as compensation, repair, replacement, price reduction, contract termination or reimbursement of the price paid, as appropriate and as available under EU law or the EU member state's national law. The possibility to seek redress is a major improvement compared to the existing Injunctions Directive 2009/22/EC.

The scope of application of the Directive covers not only the traditional consumer protection legislation, but also ensures the protection of the consumers' collective interests in such areas as data protection, financial services, travel and tourism, energy and telecommunications. The Directive will apply to representative actions brought against infringements by traders of the provisions of 66 EU instruments enumerated in its Annex I.

United Kingdom

UK Enterprise Act 2002, Part 8, section 217 (Enforcement Orders) allows consumer protection enforcement agencies to apply for a court order designed to change the business's conduct in order to end the infringement. The order must both indicate the nature of the conduct to which the finding relates and (unless the order is based on a finding that conduct amounting to a Community infringement is likely to occur), direct the business not to:

a. continue or repeat the conduct

b. engage in such conduct in the course of his business or another business

c. consent to or connive in the carrying out of such conduct by a body corporate with which he has a special relationship within the meaning of s. 222(3) of the Act. (i.e. a relationship in which the person is a controller of the body corporate, or a director, manager, secretary or other similar officer, or a person purporting to act in such a capacity.)

As provided by section 218 (Interim Orders), an interim enforcement order may be made on the basis of an allegation made by the consumer protection enforcement agency and without determination of the facts on a final basis. The safeguards for this are, firstly that the court must still conduct some assessment of the facts to determine the likelihood of the allegation in order to satisfy section 218(1)(b) i.e. that if the application had been an application for an enforcement order it would be likely to be granted. This places an obligation of disclosure on the consumer protection enforcement agency. Secondly, the court must be satisfied that there is a genuine need for urgency in prohibiting the conduct.

Section 219 (Undertakings) confers powers on both the courts and the consumer protection enforcement agency to accept undertakings from the business in lieu of an order. These provisions are accessible where the consumer protection enforcement agency believes that an infringement has occurred, is occurring or will occur. As agreement with the business can be reached before the commencement of proceedings, with the cost savings associated with this, undertakings can be used by consumer protection enforcement agencies to encourage businesses to go above and beyond what would have been required to comply with an enforcement order (i.e. ceasing the conduct): section 219(5ZA) provides that a section 219 undertaking may include further undertakings to take enhanced consumer measures (see below for details).

All of the above provisions include an obligation on the business to publish in such form and manner, and to such extent as the court thinks appropriate for the purpose of eliminating any continuing effects of the infringement, both the order/undertaking and a corrective statement.

Sections 219(A)-(B) (Redress) provide for enhanced consumer measures, which were introduced to the Enterprise Act 2002 by the Consumer Rights Act. Their intention is to enable a range of measures which result in practical action by the business to be attached to the enforcement orders and undertakings. They include, amongst other measures, redress for consumers who have suffered loss. The measures in the redress category are:

a. measures offering compensation or other redress to consumers who have suffered loss (or otherwise been affected) as a result of the conduct which has given rise to the enforcement order or undertaking,

b. where the conduct referred to in paragraph (a) relates to a contract, measures offering such consumers the option to terminate (but not vary) that contract,

c. where such consumers cannot be identified, or cannot be identified without disproportionate cost to the subject of the enforcement order or undertaking, measures intended to be in the collective interests of consumers.

The award of enhanced consumer measures is subject to the safeguard that they must be 'just, reasonable and proportionate'. This implies a balancing exercise by the consumer protection enforcement agency of the likely costs and benefits. In particular, in the case of redress measures these are available only if the consumer has actually suffered loss, and secondly the cost of implementation of the redress (excluding the “administrative” costs, which are not defined) does not exceed consumer losses.

Under section 220, failure to comply with an order or undertaking gives rise to contempt of court proceedings, whereby courts have power to exact penalties including fines and imprisonment. By contrast, EU legislation provides for a power to order payment of fines for non-compliance directly.

Considerations and good practice tips

Some countries may have explicit restrictions that only enable their enforcement authorities to act when a specific consumer is harmed, which go further than the distinction of whether the consumer is domestic or foreign (e.g. the consumer is of a specific nationality). Where possible, countries may consider ways to avoid or mitigate such clauses, which may limit cross-border enforcement co-operation and may make it difficult to act before harm takes place.

Area III: Co-operation practices

Guiding principle 7: Notification and alerts

> The 2003 Cross-border Fraud Recommendation states that Adherents and their consumer protection enforcement agencies should "develop ways to promptly, systematically and efficiently notify consumer protection enforcement agencies in other Member countries of investigations that affect those countries, so as to alert them of possible wrongdoing in their jurisdiction, simplify assistance and co-operation under these Guidelines and avoid duplication of efforts and potential disputes." (Part IV, A). It further states that Adherents should "strive to improve the abilities of consumer protection enforcement agencies to share information within timeframes that facilitate investigations of matters involving fraudulent and deceptive commercial practices against consumers, subject to appropriate safeguards" (Part IV, B).
>
> The 2016 E-commerce Recommendation provides that Adherents should "Improve the ability of consumer protection enforcement authorities and other relevant authorities, as appropriate, to co-operate and co-ordinate their investigations and enforcement activities, through notification, information sharing, investigative assistance and joint actions" (Part Three, Para 54 (ii)).

Sources: 2003 Cross-Border Fraud Recommendation, Part IV, A, B; 2016 E-commerce Recommendation, Part Three, Para 54 (ii); also relevant to UN Guidelines for Consumer Protection, Paragraphs V.A. 15, V.I.; 79 (a), 82,88, 90.

Rationale

Providing consumer protection enforcement agencies with the legal authority to notify foreign counterparts of specific and detailed information about businesses and associated individuals allows consumer protection enforcement agencies to refer investigative targets to another agency when the receiving agency may be better placed to undertake an investigation. It may also facilitate, particularly when the providing agency has already launched an investigation, concrete, practical investigation and case-specific co-operation, such as exchanging information, obtaining evidence for each other, and coordinating on parallel or complementary proceedings.

Examples

I. Case examples

Colombia

The SIC launched an administrative enforcement investigation against a multi-national business selling mobile phones worldwide, which appeared to provide misleading information to consumers about the phone's operational system updates and its implications in the device's performance. The company claimed that the SIC was the only agency in the world that was gathering information about its conduct related to this matter. However, through ICPEN the SIC formulated a request for information in order to determine if the company's statements were true, and asked ICPEN members if any was investigating or had investigated this same or a very similar case. An ICPEN member raised its hand in response to the request for information. Both agencies had a phone conversation where they explained the case they had in their jurisdiction and how they had proceeded. After this conversation, the SIC was able to identify common elements and was able to use the information as an internal strategic component of the investigation by following the recommendations provided.

Japan

Viagogo, a company based in Switzerland, set up a secondary ticket sales website in Japanese directed at consumers in Japan. The Japanese Consumer Affairs Agency (CAA) determined viagogo had caused consumer detriment through false and exaggerated advertisements and misrepresentation. The CAA shared information with the relevant Swiss authority regarding the CAA's investigation into viagogo for its conduct in Japan. The Swiss authority acknowledged the information shared by the CAA, and informed the CAA that Google had banned viagogo from advertising on their search engine. The CAA also notified the Swiss authority when it issued a warning to consumers regarding viagogo's conduct on 13 September 2019. Following the CAA investigation, viagogo undertook a corrective action plan to correct its official Japanese website by 30 September 2019.

Peru

During the Covid-19 pandemic, some businesses organised several "Cyber Wows" – marketing campaigns involving online sales promotions of goods and services, to encourage consumers to buy them. The Technical Secretariat of Indecopi organised constant monitoring of these campaigns in order to ensure that they complied with advertising and consumer regulations, with a focus on whether advertised discounts could be misleading consumers. The US FTC provided documents and information to the Technical Secretariat, which assisted it in initiating, in 2020, 15 preliminary investigations about allegedly deceptive pricing and 7 subsequent ex officio procedures.

In 2018, the head of the Peruvian tourism guild reported that platforms such as Booking.com did not list the total final prices to consumers on its website, as the prices did not include taxes (VAT). Indecopi considered this was potentially in breach of Peruvian consumer protection law, which states that sellers must indicate the total price of their services, inclusive of taxes, commissions and applicable charges. Yet as Booking.com did not have an address in Peru, Indecopi found it difficult to obtain answers to its enquiries. As the company's headquarters is in the Netherlands, Indecopi contacted the ACM asking for its assistance in contacting the company. This co-operation was possible thanks to Indecopi's participation in ICPEN working groups, allowing it to share best practices and information. The ACM's initial contact with the company led to a subsequent meeting between Indecopi and Booking.com's Latin American regional compliance officer, following which the pricing on the website was ultimately modified to comply with Peruvian consumer protection law.

Example from the privacy area

In the US FTC's action against Ruby Corp, involving the Canada-based adult dating website Ashley Madison, which had members in more than fifty countries, the FTC's early notification of its investigative interest to Canada's Office of the Privacy Commissioner and Australia's Office of the Information Commissioner enabled the FTC to coordinate its investigation closely with those authorities. The FTC charged the dating website's operators with deceiving consumers and failing to protect customer information in 36 million users' accounts. In 2016, a court settlement required the defendants to implement a comprehensive data-security program and pay a total of USD 1.6 million to settle FTC and state actions. Separately, the Office of the Privacy Commissioner of Canada and the Office of the Australian Information Commissioner contributed to the FTC's investigation and reached their own settlements with the company. The three agencies won an award from the ICDPPC (now the Global Privacy Assembly) for this co-operation, which cited the agencies' work as "a model on how to achieve cross-border co-operation in privacy enforcement".

II. Statutory examples

European Union

Article 26 of the CPC Regulation requires a competent authority to notify without delay the European Commission and other competent authorities concerned of any reasonable suspicion of an infringement covered by the Regulation that may affect consumes' interests in other EU member states and that is taking place in its territory. The European Commission is also required without delay to notify the competent authorities and single liaison offices concerned of any reasonable suspicion that an infringement covered by this Regulation has occurred.

When issuing an alert the competent authority or the European Commission shall provide information about the suspected infringement covered by this Regulation, and in particular, and, where available, the following:

(a) description of the act or omission that constitutes the infringement;

(b) details of the product or service concerned by the infringement;

(c) the names of the member states concerned or possibly concerned by the infringement;

(d) the identity of the trader or traders responsible or suspected of being responsible for the infringement;

(e) the legal basis for possible actions by reference to national law and the corresponding provisions of the Union legal acts;

(f) a description of any legal proceedings, enforcement measures or other measures taken concerning the infringement and their dates and duration, as well as the status thereof;

(g) the identities of the competent authorities bringing the legal proceedings and taking other measures.

Under the new CPC Regulation, the alerts are issued in practice in the new electronic database, available to the EU/EEA competent authorities. When issuing an alert, the competent authority or the European Commission may ask competent authorities and the relevant single liaison offices to verify whether, based on information that is available or easily accessible, similar suspected infringements are taking place in the territory of those other member states or whether any enforcement measures have already been taken against such infringements in those member states. Those competent authorities of other member states and the European Commission shall reply to the request without delay.

Example from the product safety area – European Union

In the area of non-food product safety, the EU's Rapid Alert System (Safety Gate/RAPEX) allows participating countries to quickly exchange information on dangerous products and take follow-up measures. Based on the EU-Canada Comprehensive Economic and Trade Agreement (CETA) and an administrative arrangement of November 2018, the EU and Canada have developed an automated exchange of information on dangerous consumer products between the EU's Safety Gate/RAPEX system and Health Canada's RADAR system. The exchange between the two systems includes non-publicly available information on dangerous products and enforcement measures taken.

Example from the product safety area – Mexico

The Federal Consumer Protection Law of Mexico, Article 24 paragraph XXIII and Article 25 BIS paragraph VII, gives Mexico's consumer protection authority, Profeco, the power to issue recalls and let consumers know about alerts issued by other authorities about products or services that are risky or harmful. Furthermore, the recently introduced Bylaw of the Federal Consumer Protection Law provides, in Article 70 paragraph IV, Profeco with the power to issue recalls when other authorities, domestic or foreign, publish their own recalls about risky products sold in Mexico, or similar products.

Considerations and good practice tips

When possible, consumer protection enforcement authorities should provide information about suspected wrongdoing, including details about businesses and associated individuals under investigation, at as early a point in the investigative process as possible. This would allow for more effective co-operation, including on information sharing, evidence gathering, and other assistance. It could also help agencies coordinate the timing of possible enforcement outcomes or public announcements, consistent with agencies' enforcement models and priorities.

When considering notifications and alerts, it is also important to reflect on issues such as IT tools for these notifications and alerts and their interoperability, including language issues and common classification. The EU CPC Regulation allows external entities, such as consumer or trader associations (designated to do so by EU member states or by the European Commission) and European Consumer Centres to post alerts ("external alerts") in the CPC IT system to signal potential infringements. This requires additional technical adaptation to ensure limited access to the system for such entities but has the advantage of enabling consumer and trader organisations to more directly assist enforcers in detecting breaches of consumer laws across the EU.

Guiding principle 8. Information and evidence sharing

The 2003 Cross-border Fraud Recommendation states that Adherents should provide for "Effective mechanisms to adequately investigate, preserve, obtain and share relevant information and evidence relating to occurrences of fraudulent and deceptive commercial practices." (Part IV, A). It further states that Adherents should "work towards enabling their consumer protection enforcement agencies to share the following information with consumer protection enforcement agencies in other Member countries in appropriate instances:

1. Publicly available and other non-confidential information.
2. Consumer complaints.
3. Information about addresses, telephones, Internet domain registrations, basic corporate data, and other information permitting the quick location and identification of those engaged in fraudulent and deceptive commercial practices.
4. Expert opinions, and the underlying information on which those opinions are based. And
5. Documents, third-party information, and other evidence obtained pursuant to judicial or other compulsory process" (Part IV, B).

The 2016 E-commerce Recommendation provides that Adherents should "Improve the ability of consumer protection enforcement authorities and other relevant authorities, as appropriate, to co-operate and co-ordinate their investigations and enforcement activities, through notification, information sharing, investigative assistance and joint actions" (Part Three, Para 54 (ii)).

Sources: 2003 Cross-Border Fraud Recommendation, Part IV, A, B, 2; 2016 E-commerce Recommendation, Part Three, Para 54 (ii).

Rationale

Providing consumer protection agencies with the authority under their own law to share information and evidence and information with foreign counterparts serves an important public interest. Gathering information to spot trends in marketplaces that extend beyond borders is more difficult without such information sharing. Sharing information about particular investigations and cases becomes more critical

as wrongdoers, victims, witnesses, third parties, evidence, and assets can increasingly be spread across jurisdictions. Coordinating investigations across borders also requires sharing information, and sometimes information sharing is necessary even to find out where in the world a business is located.

One highly useful category of information to share is consumer complaints. Combining complaint information enables consumer protection enforcement agencies to see the bigger picture of complaint trends, helps to focus resources where there is an indication of particularly widespread or substantial harm, and even helps consumer protection enforcement agencies resolving individual complaints to distinguish between single disputes and a larger pattern of systematic wrongdoing. Complaint sharing also can speed up the investigation process by providing consumer protection enforcement agencies with ready potential witness lists in a particular investigation. Sharing consumer complaint information can be particularly important in cases where victims are located in many countries, and therefore complain to many different agencies; without information sharing it can be difficult to determine the magnitude of a particular business practice or the magnitude of resulting harm. Because a number of jurisdictions restrict the sharing of complaints with consumer's personal data, some important information may not be available to counterpart consumer protection enforcement agencies. Accordingly, consumer protection enforcement agencies can develop protocols to ensure the flow of such information when it is necessary for the public interest while complying with privacy and data protection laws.

Sharing information about particular business is also crucial, especially in cases with a cross-border component. It may otherwise be difficult to obtain information about the nature of a business being investigated. Examples of such information include corporate records, which may or may not be publicly available; information about past business activities in another jurisdiction; information about legal proceedings in another jurisdiction, which can sometimes be challenges to the same business practices being investigated; and records already obtained from a business in another jurisdiction, which may provide evidence of the same practices being investigated elsewhere.

The sharing of expert opinions, and the underlying evidence on which those opinions are based, can also serve an important public interest. In some consumer protection cases, for example, what is at issue is the presence or absence of substantiation for a business's advertising claims. Those same claims are often made in various jurisdictions. Expert opinions can be key evidence in determining substantiation, yet can be time-consuming and expensive to develop. Sharing them with other consumer protection enforcement agencies addressing the same advertising claims can make it significantly more cost-effective for consumer protection enforcement agencies in multiple jurisdictions to pursue such claims, with corresponding benefits to consumers.

Sharing information on the identities and whereabouts of businesses and their principals becomes increasingly important in a digital marketplace. Sometimes, without sharing information consumer authorities cannot even identify who is behind a website, or where in the world they are located. Without that information, it can be extremely challenging for consumer protection enforcement agencies to develop effective remedies or even get an investigation started.

Examples

I. Case examples

Colombia

The SIC has assisted consumer protection agencies across North, Central and South America, especially in relation to businesses operating across the region but located in one country. This is the case of Open English, a company based and registered in the United States but operating online in most of the countries in the region. In this case, the Chilean consumer protection authority (SERNAC) launched an investigation into Open English on the basis of over a hundred consumer complaints against the company. The authority

made a request for information and enforcement action to the members of the Ibero-american Forum of Consumer Protection Governmental Authorities (FIAGC) and to the US FTC. The SIC co-operated by sharing consumer complaints, with redacted personal data in accordance with confidentiality and data protection laws, to assist the Chilean authority construct a stronger case.

II. Statutory examples

Canada

In Canada, the Competition Act ("Act") provides for the sharing of information with foreign authorities under certain circumstances. One of the relevant sections of the Act, section 29, is discussed below.

Section 29, known as the Confidentiality provision, allows the CBC to communicate in specific circumstances confidential information with foreign authorities to address a matter under the Act. Section 29 effectively draws under its protection nearly all information that is provided to or obtained by the CBC in the course of executing its mandate under the Act. This provision provides the CBC with the discretion to communicate information in four limited circumstances:

- communication of information to a Canadian law enforcement agency
- communication of information for the purposes of administration or enforcement of the Act
- communication of information that has been made public or
- communication of information when it has been authorised by the person who provided the information.

For the purposes of the administration or enforcement of the Act, the CBC may communicate confidential information to foreign authorities in order, for instance, to obtain enforcement assistance from foreign law enforcement authorities or to coordinate enforcement actions with foreign law enforcement authorities.

In all cases where confidential information is communicated to a foreign authority, the CBC seeks to maintain the confidentiality of the information through either formal international instruments or assurances from the foreign authority. The CBC also requires that use of the confidential information by the foreign authority be limited to the specific purposes for which it is provided. The relevant text of the section is as follows.

> 29 (1) No person who performs or has performed duties or functions in the administration or enforcement of this Act shall communicate or allow to be communicated to any other person except to a Canadian law enforcement agency or for the purposes of the administration or enforcement of this Act
>
> (a) the identity of any person from whom information was obtained pursuant to this Act;
>
> (b) any information obtained pursuant to section 11, 15, 16 or 114;
>
> (b.1) any information obtained under any of sections 53.71 to 53.81 of the Canada Transportation Act;
>
> (c) whether notice has been given or information supplied in respect of a particular proposed transaction under section 114;
>
> (d) any information obtained from a person requesting a certificate under section 102; or
>
> (e) any information provided voluntarily pursuant to this Act.
>
> (2) This section does not apply in respect of any information that has been made public or any information the communication of which was authorized by the person who provided the information.

European Union

Beyond exchange of mutual assistance requests in the IMI (Internal Market Information) system, under the CPC Regulation EU member states and the European Commission gather and exchange market-monitoring intelligence in a speedy manner, which allows the CPC network to prioritise their activities under the CPC Regulation and to promptly adapt priorities according to emerging market trends. Enforcement priorities, following consultation with all EU/EEA authorities are proposed in a two-year cycle, looking at short- (i.e. 6 months), medium- (1 year) or long-term (2 year) periods, and reviewed on an annual basis. In order to inform the public about the most concerning market trends, to address concrete compliance issues and to raise awareness on the work of the CPC network, the European Commission publishes an overview of the enforcement priorities on its website.

In order to have a more clear picture of problems experienced by consumers EU and EEA authorities launched a pilot project "Consumer Complaints Watch", that would allow transferring large unstructured data of the individual consumer complaints from all EU/EEA counties into trends, emerging issues and other valuable policy insights using advanced text analysis methods. The project should be operational in 2021.

United Kingdom

The provisions of the Enterprise Act 2002 do not prescribe or limit the type or nature of information that can be shared with overseas authorities under section 243; section 238 defines information for the purposes of the Act as any information that has been obtained by a public authority in connection with the exercise of any function that it has under Parts 1, 3, 4, 6, 7, 8 (Enforcement of Certain Consumer Legislation) of the Enterprise Act 2002.

However, the power of disclosure is subject to safeguards under the Enterprise Act: section 237 provides a general restriction on disclosure of information that relates to either the affairs of an individual or those of any business of an undertaking. This restriction applies throughout the lifetime of the individual or while the undertaking continues in existence. Disclosure of this type of information is only permitted in the circumstances that constitute an exception to the general restriction, as set out in sections 239 – 243. In the context of overseas disclosure, there are additional restrictions enlisted in section 243:

> Subsection (3) prevents the disclosure to any overseas authority of information that is held by a public authority for the purposes of Part 8 of the Enterprise Act under subsection 213(4). It also prevents the disclosure to any overseas authority of any competition information obtained under the Financial Services and Markets Act 2000 and certain sensitive commercial information (for example, information connected to market and merger investigations).
>
> Subsection (4) gives the Secretary of State discretion to prevent disclosure of information overseas if she thinks the proceedings or investigation for which the information has been requested would be more appropriately carried out by authorities in the United Kingdom or in another country.
>
> Subsection (6) sets out the considerations that a public authority must take into account when deciding whether to disclose information overseas, namely whether the reason for the request is sufficiently serious to justify disclosure, the existence of appropriate protection against self-incrimination in criminal proceedings and for personal data in the requesting country, and the existence of any mutual assistance agreements covering the information concerned with the requesting country.

Disclosure is also subject to further considerations under section 244: subsections (2) and (3) provide that, before disclosing the relevant information, a public authority must consider whether disclosure would be contrary to the public interest, and whether disclosure would cause significant harm to the interests of the business or individual to which it relates. This safeguard implies a weighing exercise on the part of the

public authority of the potential harm against the extent to which the disclosure of the information is necessary.

An additional safeguard is provided by the interplay between the provisions of the Enterprise Act and data protection law: section 237(4) expressly forbids disclosure of information which contravenes UK data protection legislation. This is particularly relevant to the power to disclose consumer complaints, including the consumer's personal data, as under data protection law consumers have the right to:

- access personal data
- have incorrect data updated
- have data erased
- stop or restrict the processing of their data
- object to how their data is processed in certain circumstances.

United States

The Federal Trade Commission Act and related rules permit the US FTC to share various categories of non-public information with foreign counterparts. In particular, section 21b(6), 15 U.S.C § 57b–2(6), added by the US SAFE WEB Act, permits the agency to share: 1) material obtained through the FTC's compulsory process powers such as a civil investigative demand (CID) (see Guiding Principle 1, above); 2) material obtained voluntarily in lieu of using a CID and marked or otherwise identified as confidential; and 3) confidential commercial information, such as trade secrets, customer lists, and other proprietary information.

Such information sharing is subject to certain conditions. For example, the FTC must obtain certification from an appropriate official of the foreign law enforcement agency that disclosed materials will be maintained in confidence and will only be used for official law enforcement purposes. The foreign law enforcement agency must set forth a bona fide legal basis for its authority to maintain the material in confidence .In addition, the foreign law enforcement agency must plan to use the materials for purposes of investigating or engaging in enforcement proceedings related to possible violations foreign laws prohibiting fraudulent or deceptive practices or other practices substantially similar to practices prohibited by any law administered by the FTC.

The FTC may also share such information if disclosure would further a FTC investigation or proceeding. The FTC has internal procedures in place that govern such information sharing, including procedures to ensure that the information sharing meets all statutory conditions and to address the sharing of information that contains consumer or other personally identifiable information. The FTC has other mechanisms to share other types of information, such as consumer complaints, with foreign law enforcement agencies, including through the econsumer.gov mechanism.

Example from the competition area

Article 12 of Council Regulation (EC) No 1/2003 of the EU provides that:

> 1. For the purpose of applying Articles 81 and 82 of the Treaty the Commission and the competition authorities of the Member States shall have the power to provide one another with and use in evidence any matter of fact or of law, including confidential information.
>
> 2. Information exchanged shall only be used in evidence for the purpose of applying Article 81 or Article 82 of the Treaty and in respect of the subject-matter for which it was collected by the transmitting authority. However, where national competition law is applied in the same case and in parallel to Community competition law and does not lead to a different outcome, information exchanged under this Article may also be used for the application of national competition law.
>
> 3. Information exchanged pursuant to paragraph 1 can only be used in evidence to impose sanctions on natural persons where:

- the law of the transmitting authority foresees sanctions of a similar kind in relation to an infringement of Article 81 or Article 82 of the Treaty or, in the absence thereof,

- the information has been collected in a way which respects the same level of protection of the rights of defence of natural persons as provided for under the national rules of the receiving authority. However, in this case, the information exchanged cannot be used by the receiving authority to impose custodial sanctions.

Considerations and good practice tips

Information and evidence sharing is essential in globalised markets. Exchanging on the main problems experienced by consumers and on priorities is an appropriate way to identify trends, emerging issues and to plan coordinated actions.

Guiding principle 9. Confidentiality

The 2003 Cross-border Fraud Recommendation states that Adherents should "take appropriate steps to maintain the necessary confidentiality of information exchanged under these Guidelines, in particular in sharing confidential business or personal information." It further states that Adherents should "respect safeguards requested by other Member countries to protect confidential business or personal information shared with them" (Part IV, F).

The 2016 E-commerce Recommendation provides that Adherents should "Strive to improve the ability of consumer protection enforcement authorities to share information subject to appropriate safeguards for confidential business information or personal data" (Part Three, Para 54 (ii)).

Sources: 2003 Cross-Border Fraud Recommendation, Part IV, F; 2016 E-commerce Recommendation, Part Three, Para 54 (ii).

Rationale

The ability to keep information received from foreign counterparts confidential is also critical for consumer agencies. Many agencies make the ability to keep information received confidential a condition for providing it, so that without this capacity an agency may not be able to get information in the first place. The ability to keep information confidential is also important to provide privacy protection for personal information received; to avoid providing premature notice of an investigation to a target that may if aware destroy evidence or secrete assets; to protect the reputation of investigational targets where there may not be any basis to allege wrongdoing; and to protect sensitive business information from leaking to competitors. Requiring that information be used only for official law enforcement purposes, and providing for confidentiality even as to the existence of investigations, similarly provides safeguards against misuse of information shared with a consumer protection enforcement agency in another country.

In practical terms, providing for the ability to limit the use and disclosure of information received from a consumer protection enforcement agency in another country may involve an exception or exceptions to a country's laws on freedom of access to government records. In many jurisdictions there may already be some applicable exceptions; in others it may be necessary to add such provisions. Jurisdictions may also have limits to these protections, as for example when information is used in a law enforcement action.

Examples

I. Case examples

Example from the product safety area

In the area of non-food product safety, the EU's Rapid Alert System (Safety Gate/RAPEX) allows participating countries to quickly exchange information on dangerous products and take follow-up measures. Based on the EU-Canada Comprehensive Economic and Trade Agreement (CETA) and an administrative arrangement (AA) of November 2018, the EU and Canada have developed an automated exchange of information on dangerous consumer products between the EU's Safety Gate/RAPEX system and Health Canada's RADAR system. Under this AA, both jurisdictions can share non-publicly available information, including confidential business information when it relates to unsafe consumer products and the AA includes appropriate safeguards to protect it. Because of differences between the two jurisdictions in the way they approach personal information, this information has been excluded from the AA and is not shared.

II. Statutory examples

Canada

Further to the provisions governing the disclosure of confidential information (presented under Guiding principle 8), the CBC published an Information Bulletin on the Communication of Confidential Information Under the Competition Act in which it provides that:

> […] [i]n all cases where confidential information is communicated to a foreign authority, the Bureau seeks to maintain the confidentiality of the information through either formal international instruments or assurances from the foreign authority. The Bureau also requires that use of the confidential information by the foreign authority be limited to the specific purposes for which it is provided.

European Union

In the framework of the EU CPC Regulation, EU and EEA consumer enforcement agencies share information via the electronic database (the IMI system) which is established and maintained by the European Commission. They can share all information in the system including detailed information on infringements and information on disciplinary, administrative or criminal sanctions. The database is accessible only to EU/EEA consumer protection authorities. The protection of personal data in the IMI system is ensured through relevant provisions in the IMI Regulation (Regulation (EU) No 1024/2012) and in the CPC Regulation. All information sent by the means of the IMI is stored for no longer than is necessary for the purposes for which data was collected and processed, but shall not be stored for longer than five years. To exchange such information with third countries' authorities, there is a need for an adequacy decision, which ensures that third countries have similar level of data protection.

United Kingdom

Enterprise Act 2002, section 243, subsections 10(a) and (b) seek to prevent information that is disclosed to overseas authorities from being further disclosed (without the permission of the UK authority from whom the information came), and to prevent the overseas authority from using the information for any purpose other than the purpose for which it is disclosed by the UK public authority and from further disclosing it to other bodies or authorities.

In the Explanatory Notes to the Act, the UK legislator recognises that subsections (10)(a) and (b) are essentially unenforceable in practice as there are no sanctions that could be taken against an overseas authority that contravenes these conditions. However, it is envisaged that the provisions might nonetheless

act as a deterrent because, should an overseas authority breach these provisions it is unlikely that a UK authority would disclose any further information.

United States

The US FTC protects the confidentiality of sensitive, nonpublic information received from businesses or consumers located domestically or abroad, or from foreign authorities, under applicable provisions of US law. For example, the FTC Act limits disclosure if the information was submitted pursuant to compulsory process or if it was submitted voluntarily in lieu of such process pursuant to a request and designated confidential. It also limits disclosure of trade secrets and confidential or privileged commercial or financial information. In addition, unauthorised disclosure of nonpublic information submitted to the FTC is subject to criminal prosecution and punishable by fines or imprisonment under the FTC Act, 15 U.S.C. § 50. Under certain circumstances, unauthorised disclosure of nonpublic agency information is subject to criminal sanction under the Trade Secrets Act, 18 U.S.C. § 1905, the Larceny Act, 18 U.S.C. § 641, and SEC Rule 10b-5.

Other US laws require the FTC to treat specific types of information as confidential, without regard to the manner in which the information is obtained. For example, US law imposes confidentiality obligations regarding certain classes of information, including personally identifiable information, maintained by federal agencies - see e.g. 5 U.S.C. § 552a (Privacy Act of 1974). There are certain, discrete circumstances in which the FTC may disclose a person's confidential information for a specific use. For example, the FTC Act does not bar the agency's use of a person's confidential information in judicial and administrative proceedings. However, the Federal Rules of Civil Procedure and FTC Rules of Practice include procedures to protect confidential information used in judicial proceedings or FTC administrative proceedings. For instance, the person providing information may seek a protective order to prevent confidential information from being made public or from being used outside the court proceeding. See Fed. R. Civ. P. 26(c); 16 C.F.R. § 3.31(d) (requiring Administrative Law Judge in FTC proceeding to issue a specific protective order).

Although the US Freedom of Information Act (FOIA), 5 U.S.C. § 552, requires federal agencies to provide access to certain existing government records to the public, the law recognises certain exceptions and excludes some records, or portions of records, from release including certain law enforcement records (e.g., certain investigatory files) including from foreign agencies. In addition, under section 21(f) of the FTC Act as amended by the US SAFE WEB Act, 15 U.S.C §§ 57b–2, the FTC may also withhold from disclosure: (i) any material obtained from a foreign law enforcement agency or other foreign government agency, if the foreign law enforcement agency or other foreign government agency has requested confidential treatment, or has precluded such disclosure under other use limitations, as a condition of providing the material; (ii) any material reflecting a consumer complaint obtained from any other foreign source, if that foreign source supplying the material has requested confidential treatment as a condition of providing the material; or (iii) any material reflecting a consumer complaint submitted to a FTC reporting mechanism sponsored in part by foreign law enforcement agencies or other foreign government agencies.

Considerations and good practice tips

Some countries have strict restrictions on confidentiality which may make sharing information challenging or even legally impossible. Countries may wish to discuss this bilaterally to see what can be done to enable information sharing while respecting relevant laws. Specific decisions or international agreements that make possible international transfer of personal data by assessing the level of protection in the respective countries might be necessary to enable workable co-operation and exchange of information.

Guiding principle 10. Co-ordination of investigations and outcomes

The 2003 Cross-border Fraud Recommendation states that consumer protection enforcement agencies should "co-ordinate their investigations and enforcement activity to avoid interference with the investigations and enforcement activity of consumer protection enforcement agencies taking place in other Member countries" (Part III, B). It further states that consumer protection enforcement agencies should "make every effort to resolve disagreements as to co-operation that may arise" (Part III, C).

The 2016 E-commerce Recommendation provides that Adherents should "Simplify assistance and co-operation, avoid duplication of efforts, and make every effort to resolve disagreements as to co-operation that may arise, recognising that co-operation on particular cases or investigations remains within the discretion of the consumer protection enforcement authority being asked to co-operate" (Part Three, Para 54 (ii)).

Source: 2003 Cross-Border Fraud Recommendation, Part III, B, C; 2016 E-commerce Recommendation, Part Three, Para 54 (ii).

Rationale

The process of investigations should be flexible enough to permit co-operation and co-ordination, both in order to reduce burdens on business in facing multiple and potentially inconsistent approaches, and to secure efficient and effective outcomes which benefit the widest possible group of consumers.

Detail of the powers

There should ideally not be a legislative barrier to co-operating with foreign consumer protection enforcement agencies merely because a consumer protection enforcement agency has already commenced enforcement proceedings against a business.

Consumer protection enforcement agencies should ideally be able, in appropriate cases, to agree a common position as to the remedies which they will seek from a business under investigation, based on their individual analysis of illegality.

Consumer protection enforcement agencies should ideally have the option to present their case collectively to the business, to request the agreed remedies be implemented, and together carry out negotiations with the business to secure an outcome.

Any outcome secured from the business as a result of a joint approach should ideally be enforceable formally in the jurisdictions of participating authorities. However, the existence of different remedies in different jurisdictions need not prevent co-operation (e.g. in the Ashley Madison case).

Examples

I. Case examples

Benefits of ICPEN membership and sweeps - Zambia and Kenya

Within the ICPEN, consumer protection enforcement agencies conduct yearly sweeps to screen the market on a specific marketing practice or phenomenon affecting consumers. The findings are used to inform agencies of the state of play, including opportunities for co-operation, and often lead to a follow-up enforcement phase. For example, following an ICPEN sweep the Competition and Consumer Protection Commission of Zambia found that there was a need for more cross-border co-operation among members,

even bilaterally, in relation to uncovering the real owners behind websites engaging in deceptive online commercial practices.

Similarly, through the ICPEN sweep, the Competition Authority of Kenya ("the Authority") was able to address consumer issues involving e-commerce firms such as unfair terms and conditions amongst others. The Authority's membership of ICPEN has also been beneficial in enhancing enforcement capacity. In particular, officers from the Authority have benefitted from enforcement manuals prepared through ICPEN, and training on consumer protection enforcement. Furthermore, the Authority developed valuable networks resulting in further support to its investigations. For example, the UK CMA provided ground support in an investigation by the Authority where a Kenyan consumer was defrauded around GBP 5 000; the ACCC provided information to the Authority on a certain vehicle brand which had been recalled in Australia and was subject to an investigation by the Authority; the US FTC has provided training to officers and provided valuable information on how to conduct e-commerce consumer related investigations.

COMESA Competition Commission and African Dialogue - Kenya

In 2018, through the COMESA Competition Commission (CCC), the Authority hosted and trained enforcement officers from the Ethiopian Trade Competition and Consumer Protection Authority. The Authority has also investigated consumer violations forwarded by CCC e.g. recalls of products such as pilchard canned fish and juice products in the COMESA region, and unconscionable terms and conditions by furniture companies still operating in the COMESA region.

Additionally, through participation in the African Dialogue, the Authority has shared its experiences with colleagues in other African countries, in ensuring that providers of digital financial services through mobile phone, apps and USSD disclose fees and charges prior to consumers undertaking a transaction. The Authority has also shared its experiences on the e-commerce sweep it conducted.

European Union - CPC network sweeps and coordinated actions

Every year the consumer protection authorities from the EU and the EEA conduct sweeps, as foreseen in the CPC Regulation, to identify breaches of EU consumer law in a particular sector. The sweeps are coordinated by the European Commission. When conducting a sweep, the competent authorities involved may use their new minimum investigation powers and any other powers conferred upon them by national law. These checks show whether traders respect EU consumer protection laws. Where the checks reveal potential breaches of EU consumer law, the consumer protection authorities contact the responsible companies and ask them to make corrections. Sweeps are normally conducted in sectors where consumer complaints or other suggest that infringements of EU laws that protect consumers' interests have occurred or are occurring. They can also be used to verify the level of compliance with new EU legislation. Recent sweeps concerned misleading sustainability claims, consumer scams related to the Covid-19 pandemic, delivery and the right of withdrawal, and drip pricing.

The CPC Regulation allows the CPC network of EU/EEA authorities to engage in coordinated actions in case of infringements which concerns more than two EU member states. These coordinated actions can be conducted under the coordination of one of the participating authorities or of the European Commission.

Examples of coordinated actions of the CPC network include actions led by:

- The European Commission, concerning proliferation of misleading offers and ads and consumer scams related to masks, sanitising gels and protective equipment found on platforms during the COVID-19 pandemic. The action obliged main online platforms to monitor and remove misleading offers and ads.
- The Danish Consumer Ombudsman, concerning the marketing of online games as free when in fact in app purchases were offered. Apple iTunes and Google Play stopped this practice and developed information on the main items that can be purchased as part of the games.

- The UK CMA, related to unclear conditions for car rentals. The five leading car rental companies — Avis, Europcar, Enterprise, Hertz and Sixt — considerably improved the transparency of their offers and handling of damages.
- The French Directorate General for Competition Policy, Consumer Affairs and Fraud Control (DGCCRF) concerning terms in social media contracts. Facebook, Twitter and Google+ updated their terms of services and implemented a dedicated procedure for consumer authorities to signal problematic content.
- The Norwegian Consumer Authority, the ACM and the Hungarian Competition Authority regarding online travel platforms Airbnb, Booking and Expedia. The booking platforms agreed to improve and clarify the way they present accommodation offers to consumers, for example, by providing adequate and complete price information (including all mandatory charges and fees).

Yellow Pages business directory scam

An example of multi-jurisdictional intelligence sharing which led to the quick identification of emerging issues, global deterrence and an effective coordinated enforcement outcome is the "Yellow Pages" directory scam. Beginning in 2010, this case involved co-operation and coordinated action across a range of authorities in different jurisdictions: the ACCC, the CBC, the US FTC, the Swiss State Secretariat for Economic Affairs, the UK National Fraud Intelligence Bureau, and the New Zealand Commerce Commission. Further details on the case are presented under Guiding principle 4.

Example from the competition area

In 2014-2015 France, Italy and Sweden conducted parallel investigations concerning parity clauses in the agreements between online hotel booking platforms and accommodation providers. The three co-operating agencies, supported by the European Commission, had very useful discussions on the substantive issues at stake, which ultimately paved the way for an alignment of their decisions to accept the same package of EU-wide commitments and to communicate that decision on the same day. On the procedural side, Italy considered it important to align its investigation timetable to ensure the continued coordination with the other agencies: the deadline for the submission of the final commitments envisaged in the Italian legislative framework was extended to allow the continuation of the discussions among the coordinating agencies and to facilitate the efforts of the undertakings concerned in dealing with several authorities to elaborate a common commitment package (OECD & International Competition Network, 2021[5]).

Example from the product safety area

In the area of non-food product safety, through Safety Gate the European Commission helps national authorities across Europe work together, pool resources and share best practices through coordinated market surveillance activities. Based on the EU-Canada Comprehensive Economic and Trade Agreement (CETA). In this context, the EU and Canada have piloted a coordinated market surveillance activity on heavy metals in children's jewellery in 2020, where participating authorities sample products sold on their respective markets according to jointly defined criteria and will share the results of the testing. In addition, the EU and Canada have implemented joint outreach activities on issues of common interest related to consumer product safety and using jointly developed messaging.

II. Statutory examples

European Union

The CPC Regulation requires authorities to coordinate and work together in case of infringements which concern more than two EU member states. It also provides for a specific procedure to tackle EU-wide infringements. The current CPC Regulation gives more powers to the European Commission in case of practices which harm a vast majority of European consumers. The European Commission can alert national authorities and coordinate their action. This is followed by negotiation with the businesses

concerned, directly at EU level. The new CPC Regulation has also formalised some steps in the coordinated action related to investigation and enforcement measures, which had become informal practice under the previous regulation, and therefore it offers a more comprehensive legal framework for such actions.

Not all member states are obliged to participate in a coordinated action. However, the new CPC Regulation sets a clear list of reasons for declining to take part in a coordinated action. When participating in the action the member state can support the action at different levels, by commenting the documents and participating in meetings with traders, or decide just by agreeing to the actions taken by other authorities. The coordinated aim is to obtain EU-level benefits and solutions for all EU consumers. When authorities work on a coordinated action related to a widespread infringement, an assessment of common issues (the common position) is agreed by way of consensus.

The procedural rules are detailed Articles 17-25 of the CPC Regulation. Article 17 of the Regulation allows EU competent authorities that are concerned with a widespread infringement or a widespread infringement with an EU dimension to take part in a coordinated action. However, competent authority shall join the coordinated action, if it becomes apparent during that coordinated action that the competent authority is concerned by the widespread infringement or the widespread infringement with an EU dimension. The reasons for refusing to take part in a coordinated actions are enumerated in Article 18 of the Regulation. Article 19 of the Regulation indicates that where appropriate, the competent authorities concerned by the coordinated action shall set out the outcome of the investigation and the assessment of the infringement in a common position agreed upon among themselves. The Regulation also indicates that the common position is communicated by the coordinator to the trader responsible for the infringement and the trader shall be given the opportunity to be heard on the matters forming part of the common position. Article 20 deals with the commitments which can be requested by the participating authorities or which can be offered by the trader on his own initiative, and which aim to cease that infringement or offer remedial commitments to consumers that have been affected by that infringement.

Article 21 details conditions under which enforcement actions can be taken. The article specifies in paragraph 1 that:

> The authorities concerned by the coordinated action shall take within their jurisdiction all necessary enforcement measures against the trader responsible for the widespread infringement or the widespread infringement with a Union dimension to bring about the cessation or prohibition of that infringement.

Where appropriate, they shall impose penalties, such as fines or periodic penalty payments, on the trader responsible for the widespread infringement or the widespread infringement with an EU dimension. The competent authorities may receive from the trader, on the trader's initiative, additional remedial commitments for the benefit of consumers that have been affected by the alleged widespread infringement or the alleged widespread infringement with an EU dimension, or, where appropriate, may seek to obtain commitments from the trader to offer adequate remedies to the consumers that have been affected by that infringement.

Enforcement measures are in particular appropriate where:

> (a) an immediate enforcement action is necessary to bring about the swift and effective cessation or prohibition of the infringement;
>
> (b) it is unlikely that the infringement will cease as a result of the commitments proposed by the trader responsible for the infringement;
>
> (c) the trader responsible for the infringement has not proposed commitments before the expiry of a time limit set by the competent authorities concerned;

(d) the commitments that the trader responsible for the infringement proposed are insufficient to ensure the cessation of the infringement or, where appropriate, to provide a remedy to consumers harmed by the infringement; or

(e) the trader responsible for the infringement has failed to implement the commitments to cease the infringement or, where appropriate, to provide a remedy to consumers harmed by the infringement, within the time limit referred to in Article 20(3).

Enforcement measures pursuant to paragraph 1 shall be taken in an effective, efficient and coordinated manner to bring about the cessation or prohibition of the widespread infringement or the widespread infringement with an EU dimension. The competent authorities concerned by the coordinated action shall seek to take enforcement measures simultaneously in the member states concerned by that infringement.

Considerations and good practice tips

Conducting sweeps on a particular sector by authorities from different countries requires important preparation and coordination (e.g. common understanding of legal and other issues among the participating authorities, preparation of common questionnaire and guidance documents, establishment of common timeframe for the performance of the sweep). In the EU, the use of a common methodology to conduct the sweep is very important as it ensures that compliance with EU law in the market/sector is assessed on the basis of comparable data. Sweeps have been found to also contribute to raising awareness on consumer laws among both traders and consumers.

In the EU, coordination of investigation and outcomes is not always easy as enforcement capacities of national authorities still differ significantly and depend greatly on several factors, such as the size of the budget allocated to enforcement activities. Some countries have more human and financial resources to participate in coordinated actions. Coordinated actions are suitable mostly for large multinational traders with large market shares. Indeed, the actions analyse specific practices of traders across a number of markets. This requires analytical capacities to scan numerous multilingual documents and websites. If traders do not co-operate, enforcement measures will have to be activated under national law of the member states, as they remain competent to enforce EU consumer law.

References

OECD (2020), *Roundtable on Legislative Initiatives to Improve Cross-border Enforcement Co-operation: Summary of Discussion*, https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/CP(2019)21/FINAL&docLanguage=En. [2]

OECD (2018), *Conclusion of the Review of the 2003 Recommendation on Protecting Consumers from Fraudulent and Deceptive Commercial Practices across Borders*, https://www.oecd.org/sti/consumer/DSTI-CP(2018)7-FINAL.en.pdf. [3]

OECD (2018), "Consumer protection enforcement in a global digital marketplace", *OECD Digital Economy Papers*, No. 266, OECD Publishing, Paris, https://dx.doi.org/10.1787/f041eead-en. [1]

OECD (forthcoming), *OECD Best Practice Principles on International Regulatory Co-operation*. [6]

OECD & International Competition Network (2021), *OECD/ICN Report on International Co-operation in Competition Enforcement*, https://www.oecd.org/daf/competition/OECD-ICN-Report-on-International-Co-operation-in-Competition-Enforcement.pdf. [5]

United Nations (2015), *United Nations Guidelines for Consumer Protection*, https://unctad.org/en/PublicationsLibrary/ditccplpmisc2016d1_en.pdf (accessed on 6 May 2019). [4]

Notes

[1] More information on the database is available at https://www.ftc.gov/enforcement/consumer-sentinel-network/reports, and https://econsumer.gov. *Econsumer.gov* is an initiative of the International Consumer Protection and Enforcement Network (ICPEN), a network of more than 60 consumer protection authorities from around the world that seeks to combat cross-border fraud through enforcement co-operation. *Econsumer.gov* is a jointly sponsored website of 39 consumer protection agencies around the world, for consumers to file cross-border complaints.

[2] For example, the European Union's Consumer Protection Co-operation Network: https://ec.europa.eu/internal_market/scoreboard/performance_by_governance_tool/consumer_protection_cooperation_network/index_en.htm.

[3] The broad range of mechanisms available to countries to co-operate on enforcement is further detailed in OECD (forthcoming[6]).

[4] While the revised UNGCP were adopted in December 2015 and the revised E-commerce Recommendation in March 2016, both instruments were developed in parallel and the E-commerce Recommendation's drafts fed into the new chapter on e-commerce in the UNGCP.