

Combating Visual Identity Impersonation through the Activation of Information Security Systems in Economic Institutions in the Electronics Industry

Dr. Abdessamia Tahar ¹, Dr. Bilal Bekhouche ²

¹ Faculty of Media and Communication Sciences, University of Algiers 3 (Algeria);

Email: tahar.abdessamia@univ-alger3.dz

² Faculty of Economic Sciences, Commercial Sciences and Management Sciences, University of Tébessa (Algeria); Email: bilal.bekhouche@univ-tebessa.dz

Received: 15/02/2026 ; Accepted: 09/06/2026 ; Published: 09/09/2026

Abstract

The electronic device manufacturing sector is witnessing a marked increase in the phenomenon of visual identity impersonation of economic institutions, through the imitation of logos and trademarks, and the simulation and counterfeiting of the visual appearance of original products, thereby threatening consumer trust, affecting brand reputation and credibility, and increasing institutions' need to deploy effective information security systems to detect manifestations of impersonation, imitation, and counterfeiting and to limit their effects.

The study relied on the descriptive-analytical method and the multiple case study method, using a purposive sample composed of 24 global companies operating in the electronic device manufacturing sector, which were shown to actually rely on information security mechanisms or systems and technical and digital measures to confront manifestations of visual identity impersonation and the imitation of their products and trademarks. Data collection was based on official documents, institutional reports, and the official websites of the companies under study, with the aim of analyzing the nature of the threats, the detection and protection mechanisms adopted, and the level of deployment of information security techniques in confronting this phenomenon.

The results showed that imitation, counterfeiting, and the impersonation of visual identity elements represent a growing challenge for the majority of globally renowned institutions, which has driven them to adopt varied mechanisms to confront it, including security technologies embedded in the structure of products or their packaging, digital solutions for verifying product authenticity, identification and tracking systems, mechanisms for monitoring and detecting illegitimate products or channels, in addition to digital and legal measures to protect trademarks. The results also revealed a clear disparity in the level of activation of these mechanisms, depending on the nature of the institution's activity, the type of its products, and the level of exposure of its visual identity and products to imitation and counterfeiting.

Keywords: Visual identity impersonation; information security; counterfeiting; imitation; trademark.

I. Introduction

The electronics industry today is considered one of the most globalized and interconnected economic sectors in the world, as production and supply chains are intertwined across dozens of countries. According to statistics from the CompaniesMarketCap website, there are 163 companies

worldwide operating in the electronic device manufacturing industry with a market capitalization exceeding one billion dollars; and although these statistics are constantly changing, they reflect the scale of the massive investments deployed by these institutions in order to win a share of the market and secure their position in the world economy. A study by (Ou, Yang, Liu, 2024) showed that the global production pattern of the semiconductor industry is characterized by intense trade interdependence among the major economies, with a clear shift in the center of gravity toward Asian economies, whose share of integrated-circuit trade rose by more than 80% during the period from 2001 to 2019, reflecting the pivotal role played by global economic institutions operating in this sector.

This geographic expansion is accompanied by an increasing reliance on digital channels for communication and commercial dealings among manufacturers, suppliers, and customers, which has made the visual and digital identity of these institutions a highly sensitive strategic asset, and at the same time an attractive target for malicious actors seeking to exploit it; impersonators breach legitimate websites or register new domains with the aim of hosting pages that impersonate the visual identity of trusted institutions, in order to lure victims into disclosing their personal or financial information (Agarwal, Vasek, 2026). It is also noted that attackers disproportionately prefer the infrastructure of old, highly trusted domains, as these are perceived by users as more credible and less likely to be detected and blocked by automated security-filtering systems (Agarwal, Vasek, 2026).

This phenomenon falls within a broader context, as counterfeit products represent a growing threat to companies around the world (INTA, 2023), and almost any product can be counterfeited, including electronic devices (Pecht, Tiku, 2006); the annual value of global trade in counterfeit products amounts to hundreds of billions of dollars (OECD, EUIPO, 2025; Frontier Economics, 2017). The effects of this phenomenon are not limited to lost sales and profits, but also include opportunity costs resulting from reduced investment in research and development, lost returns and royalties, reduced employment levels, damage to the institution's reputation and market share, as well as defensive costs incurred in confronting these threats (Cuntz, Qian, 2021; INTA, 2023; OECD, 2008; Wilson et al., 2016).

The most effective responses to these threats consist of integrating anti-counterfeiting activities within broader strategies for protecting visual identity (Wilson, 2022). Although this protection extends to a wide scope including the management of institutions' image and reputation, the legal protection of identity and other intellectual property rights (IPR) represents a fundamental strategic element within it (M'zungu et al., 2010; Maurya, Mishra, 2012). However, product-counterfeiting crimes remain among the most complex and difficult impersonation-related problems to address; unlike crimes assumed to be victimless, they affect almost everyone in one way or another: they impact consumers' health and safety, reduce the profits of visual identity owners and their capacity for innovation, lead to a decline in tax revenues while increasing prevention and enforcement costs, fuel organized crime and terrorism, undermine national security, and lead to job losses (Wilson, Kinghorn, 2015). Numerous factors contribute to shaping the opportunities for the spread of this phenomenon, including the global economy, ease of internet access, technological progress, consumerism and demand for low prices, cultural variation in the level of acceptance of these practices, high profit margins, low probability of detection and punishment, and lack of awareness among various stakeholders (Wilson, Kinghorn, 2015); this explains the continuous attention given by international professional conferences, such as the

International AntiCounterfeiting Coalition (IACC), Interpol, and Underwriters Laboratories, to issues of enforcing the protection of visual identity and intellectual property rights since 2013.

These dynamics are of particular importance for companies operating in the global electronics industry, given their heavy reliance on geographically distributed, multi-tiered supply chains, and on trusted digital interactions among manufacturers, suppliers, and customers. The literature specialized in supply chain management has identified cybersecurity as an emerging and pressing challenge for this sector, citing the sophisticated, state-sponsored breach disclosed in December 2020 (the SolarWinds breach) — an American company specialized in developing IT-management software — as evidence of systemic fragility across interconnected manufacturing and technology networks (Melnik, Schoenherr, Speier-Pero, Peters, Chang, Friday, 2022). Within these supply chains, device manufacturers occupy a particularly sensitive position, as security vulnerabilities introduced during the design or production stage can later be transmitted to end customers and partner institutions (Latsiou, Lambrinoudakis, 2026).

The importance of this sensitive asset (i.e., visual identity) is manifested in its being the distinctive and unique communicative process through which the institution defines itself, as it moves the individual, through its visual discourse, from the stage of perception to the stages of persuasion, action, and preference. It visually reflects the strong values and essential characteristics of the institution and its products through its visual components such as the logo, name, and colors. Visual identity is also manifested through office stationery — such as business cards, envelopes, correspondence paper, disc/record sleeves, pens, and all office supplies — as well as print advertisements, television commercials, the website, transport buses and company vehicles, the building or display windows, in addition to packaging, which plays an important role in displaying it (Bosch, 2006).

In contrast, the concept of information security revolves around determining access to data and its disclosure, by preventing outsiders and non-members of the institution from tampering with or disposing of information without authorization; the objective of any security system is to protect the institution's information by reducing and managing risks from any attack that could affect the institution financially or in terms of reputation.

Despite growing recognition of information security management system frameworks as a governance response to security threats, and despite documented evidence of visual identity impersonation through phishing and supply-chain fragility in technology-intensive sectors, attention to how global economic institutions in the electronics industry specifically deploy information security systems to combat visual identity impersonation remains limited.

The gravity of this phenomenon is embodied on the ground in the experience of global institutions operating in electronic devices, which have actually attempted to adopt information-security measures that protect their visual identity, or at least reduce the risk of its impersonation — institutions that have incurred losses amounting to billions of dollars as a result of the theft of their designs, marks, shapes, and colors by other companies (competing or fictitious companies operating covertly) that feed off others' reputations in their visual identity, by imitating the institution's profile, background, general appearance, or content in a way that makes it resemble another institution enjoying a good reputation and a mental image firmly established in the perceptions of its community. Since these global institutions enjoy a reputation that was not built overnight but through long years of positioning in the marketplace and

investing money in research and development, they have made the preservation and management of their information security using security systems a matter of paramount priority, aiming to extend control over their official communication networks and prevent them from being breached from outside the institution or having their data tampered with.

Hence this study aims to shed light on combating visual identity impersonation through the activation of information security systems in economic institutions, the risks threatening their information security, the reasons calling for continuous reflection and permanent vigilance to guard against this phenomenon, in addition to the set of international and national protective measures and mechanisms capable of limiting these threats.

From this, the following four questions arise:

- What explains the difficulty of determining the true scale of the phenomenon of visual identity impersonation within global economic institutions in the electronics industry, despite some institutions relying on monitoring systems that reflect only the minimum extent of the actual phenomenon?
- Why do some economic institutions remain confined to reactive (purely legal) strategies in confronting the impersonation of their visual identity, while other companies adopt comprehensive proactive approaches — and what determines this difference despite both parties having information security systems available?
- How can an information security system move from being an isolated technical tool to becoming an integrated pillar within a holistic approach to protecting visual identity, one that engages senior management, employees, customers, and suppliers simultaneously?
- How do institutions balance reliance on their internal information-security capabilities with the use of external service providers (such as digital monitoring and legal support) to combat the impersonation of their visual identity, and what risks does this option pose?

2. Methodology :

This study relied on the descriptive-analytical method, which is based on describing the phenomenon of visual identity impersonation as it manifests in the reality of global economic institutions, then analyzing the data related to the security measures adopted by these institutions to confront it. This method allows for linking the theoretical framework of the concepts of visual identity, information security, and impersonation with the real-world data extracted from the institutions under study.

The study also relied primarily on the multiple case study method, which is based on examining a number of units (institutions) in depth in order to identify the actual practices they apply in the field of activating information security systems to combat visual identity impersonation. This method allows for comparisons among the studied cases, and for extracting the patterns and common denominators in the security procedures and technologies adopted, without the need for direct intervention in the environment of the cases under study, relying entirely on documented and published data.

The study population consists of global institutions operating in the electronic device manufacturing sector, while the study sample consists of 24 global institutions selected using purposive sampling — a non-probability sampling method based on selecting cases according to a predetermined criterion. This criterion consists of these institutions having actually activated information security systems dedicated to combating the impersonation of their visual identity, and having documented and

published data available about them that can be referred to through their official reports, websites, or reliable secondary sources — which ensures the availability of the necessary data for each case, and makes the sample suitable for achieving the study's objectives and answering its research questions and hypotheses. These institutions varied among manufacturers of smartphones and computers, semiconductor and electronic-component companies, printing and imaging companies, and home-appliance and air-conditioning companies, reflecting the breadth of the electronic device manufacturing sector covered by the study.

Given the nature of the adopted design, based on multiple case studies, the study relied in collecting its data on multiple documentary data sources, with the aim of enhancing the validity and reliability of the results through comparison among multiple sources for the same piece of information. These sources consist, first, of content analysis, which constituted the study's main tool, whereby data were extracted from the companies' official websites, their published brand-protection and anti-counterfeiting pages, and the security and technical reports officially issued by the 24 institutions in the study sample, according to a pre-prepared analysis grid containing specific indicators — most notably digital watermarking technologies, counterfeit-detection systems via QR codes, color-shifting holographic labels, digital brand-authentication certificates, and digital visual-identity monitoring mechanisms.

The second source consists of the analysis of official documents, which included the study of security policies published by the institutions in the study sample, patents related to visual-identity protection technologies, and official press releases issued by these institutions regarding identity-impersonation incidents they have faced and the measures they have taken to confront them. The third source consists of secondary sources, which included previous studies and literature relevant to the topic, international reports issued by bodies specialized in information security and intellectual-property protection, in addition to the databases and public records of the United States Patent and Trademark Office.

The data collected from these multiple sources were subjected to a thematic analysis process based on classifying the data extracted from each case within unified analytical themes — including the type of security technology adopted, the date of its activation, and its effectiveness in reducing visual identity impersonation — then conducting a comparison across the 24 cases in order to extract the general findings and common patterns that answer the study's research problem and test its hypotheses.

Table 1: *The economic companies relied upon in the analysis process.*

Institution	Documented Evidence	Source Type
Apple	Embedded software authentication (licenses, warranty) + legal action against counterfeiters	Specialized article
Samsung	QR verification system + IMEI check + Knox feature via samsung.com	Official website
Cisco	Trustworthy Technologies + SUDI certificate + holographic security labels + Brand Protection team	Multiple official websites (Cisco.com)
Microsoft	Holographic COA label + official "How to Tell" website	Official website

HP	Official ACF program + variable visual security labels + verification QR code	Official websites (several countries)
Intel	Official Assured Supply Chain (ASC) program	Official website + specialized report
LG	Verification system via SMS and official website (Product Validation)	Official websites
Sony	Official page for detecting hologram and logo counterfeiting	Official website
Huawei	Official anti-counterfeiting code-check system (c-ver.huawei.com)	Official website
Xiaomi	Official verification website (mi.com/c/verify) + dedicated patent (US9426130B2)	Official website + USPTO
Dell	Official "Detect Product" tool (Service Tag) + 2017 UL Brand Protection award	Official website + UL report
Philips	philips.com/original + COA certificate + QR code	Official website
Panasonic	Official Brand Protection page + "No Counterfeit Products" campaign	Official website
Amazon	Official Transparency program + Project Zero	Official website
STMicroelectronics	Official page on the use of NFC anti-counterfeiting technology	Official website
Texas Instruments	Official Anti-counterfeit page + Counterfeit Validation Form	Official website (ti.com)
Broadcom	Official "Counterfeit & Gray Market Awareness Statement" page	Official website
Bosch/BSH	Origify system + Secure Product Fingerprint + KeySecure Code	Official website (multiple)
Google	Official Device Authenticity system (anti-counterfeit label + QR)	Official website (store.google.com)
Anker	Official verification system (anker.com/verify) with a 16–20 digit security code	Official website
Canon	Official anti-counterfeiting hologram + counterfeit-battery recognition technology	Official Canon websites (multiple regions)
Epson	Official Epson Genuine Ink app + advanced thermal/optical hologram	Official website
Brother	Hologram + QR + ID number + official verification tool	Official website (brother-usa.com)

Daikin	Air conditioning — official hologram with QR and an 8-digit code + official anti-counterfeiting department (daikin.com)	Official website
---------------	--	------------------

Source: Prepared by the researcher.

3. Theoretical Framework :

3.1. Visual Identity in Economic Companies :

The visual identity of the institution enjoys growing attention in the literature of organizational communication and brand management, being considered one of the fundamental components that the organization uses to express itself and highlight its characteristics before various stakeholders. Visual identity is not limited to individual design elements, but consists of a set of symbols and graphic elements that express the essence of the organization, and that contribute to enhancing its visibility, distinctiveness, authenticity, and consistency (Bosch, 2005). Visual identity is also linked to the institution's strategic communication, particularly in terms of its authenticity and its ability to express the organization's identity (Johansen, Gregersen, 2024). Hence the importance of addressing the concept of visual identity, its functions, and its role in defining the institution and distinguishing it from others.

The accelerating transformation in the digital communication environment has contributed to expanding the fields in which this identity appears; the process of visually expressing the institution is no longer confined to traditional media, but now extends across multiple communication environments and platforms, which makes the management of visual identity more closely tied to the issue of consistency across platforms and authenticity of expression. Recent literature confirms that visual identity has become a strategic subject that goes beyond the aesthetic and design dimension to dimensions of communication, identity management, and relationships with stakeholders; (Melewar, 2006) considers that corporate identity is linked to the organization's reality, strategy, philosophy, history, scope of business, and formal and informal communications, while (Bosch, 2005) shows that visual identity is an important element in the management of identity, reputation, and relationships.

Hence, the study of the visual identity of the economic institution is not limited to cataloguing its formal components, but requires understanding its communicative and symbolic functions, and how its elements are employed in building a coherent and distinguishable image of the institution, in addition to studying the mechanisms of its management and protection in a digital communication environment in which the points at which the brand appears multiply and the likelihood of the reproduction or illegitimate use of its visual elements increases. This matter acquires particular importance in light of what recent studies have found — namely, that the management of visual identity is linked to issues of consistency, authenticity, and continuity across different platforms and communicative contexts.

3.1.1. Visual Identity :

3.1.1.1. Identity :

The term "identity" did not begin to acquire a meaning referring to symbolic experiences or lived experience until the twentieth century, and credit for the spread of this meaning is largely due to the psychology developed by Erik Erikson (Laflamme, 2016). The concept of identity has received renewed attention in the humanities and social sciences, being considered one of the most important traits that

distinguish the individual and society, and one in which future aspirations are embodied — which is reflected in individuals' behavior across all fields.

This also applies to institutions: identity must be based on origins, standards, ethical principles, and social controls that give the institution an identity distinguishing it from other institutions.

Claudiu Coman considers that identity is the way in which members of an organization define who the organization is, both for themselves and for people outside the organization; the concept of identity can therefore be approached from several points of view:

On one hand, the identity of the institution is viewed as its essence — the central, distinctive thing that has continuity over time.

On the other hand, the identity of the institution is also linked to the idea of change; that is, the institution's identity is not fixed but flexible, has many functions, and does not remain the same over time, but is subject to change (Coman et al., 2021).

Louis-Jacques Dorais, for his part, considers that identity is not fixed but dynamic, emerging when it is used; identity is important because it exists everywhere, and every individual has an awareness of the identity that distinguishes them from others — which means that identity can be treated as an individual phenomenon determined mainly by the individual's construction of their personal relationship with their surrounding environment (Dorais, 2004).

3.1.2. Visual Identity :

Terminologically, visual identity is said to be a specific set of goals that the organization aspires to create and maintain by embedding them in customers' minds. When consumers search for, shop for, and consume brands, they are exposed to specific brands (Phillips, 2014); among the elements most firmly embedded in memory are logo design, color, typography, and the slogan, to which another element — voice — can be added.

In addition, a new type has emerged as a result of the outputs of modern information and communication technology, represented by dynamic (moving) visual identities (Rebelo, 2022), which have moved somewhat away from the classical principles of visual identity that, during the design process, used to focus on converting the institution's value-laden message into visual symbols through which it communicates with the general public — going beyond material interest toward an attempt to build a psychological and social relationship. Whereas a fixed visual identity preserves its core values for fear of dispersing the stereotyped identity firmly held by the public, the process of designing visual identity today has become more complex, requiring the exploration of new methods capable of dealing with various data in real time (Rebelo, 2022).

Through visual identity, an institution can be distinguished from others, since the institution's personal traits are linked to what is visually noticeable to the viewer; the institution's own visual identity plays an important role in how the institution presents itself, whether before an internal or an external audience (Bosch, 2006).

According to Kevin Lynch, visual identity is defined as "a person's ability to recognize a place as a result of its distinctiveness from others through distinguishing traits and characteristics, and an environment whose identity relies on a particular activity tends to be very strong, in that users usually share in and interact with such distinctive activities." This means that Lynch attempted to link identity,

people, and the physical environment through the mutual relationship between people and the physical environment, since feeling and perception differ from one person to another depending on each person's situation and location; nevertheless, there are certain physical considerations that different people perceive in the same way when they experience the same place or location (Lynch, 1984).

Visual identity goes far beyond a mere trademark, as it constitutes a fully integrated set of structural elements. These elements include at least an identifying symbol, such as a logo or brand mark, in addition to a diverse set of colors and typefaces. In the past, symbols were used permanently to distinguish institutions' identities; however, the scope of influence of corporate and institutional visual identities has evolved over time, especially with the expansion of the scope of business and activities during the 1950s. This development contributed to the strengthening and emergence of visual identity systems in the sense we know today (Rebelo, 2022).

The visual identity of institutions rests on discerning the satisfactions of the target audience and knowing whether the institution is positioned in this audience's memory relative to its competitors, in order to capture a larger market share; this approach may change over time from the traditional method of advertising through direct communication to online platforms in order to reach a larger audience, in addition to the performance of marketing services as a metric measuring certain market strategies in terms of profitability, sales growth, customer loyalty, market share, and others (Adebayo, 2019).

3.2. Dimensions of Visual Identity in Economic Institutions :

In the process of forming their visual identity, economic institutions are concerned with a set of dimensions related to the institution's historical and cultural dimension and the social environment surrounding it, or to the product it wishes to market within a particular social environment. For this reason, decision-makers must take all these dimensions into account when beginning the design and graphic process, since these dimensions contribute to embodying the institution's personality and identity before the public and customers, and play a prominent role in creating a positive image of the institution and enhancing recognition of it. Three main dimensions can be identified with which visual identity deals in economic institutions:

3.2.1. The Historical and Cultural Dimension :

This refers to the historical record and the developments the brand has gone through over time; identity, from a historical point of view, is very important, especially for long-established institutions, because it provides an implicit account of the brand's trajectory and heritage from its founding to the present time, contributing to building the identity and values the brand represents. Brands carry within their history experiences and events that have shaped their reputation and their interaction with the public, and the elements of a brand's historical dimension include the following:

- Founding and beginnings: the date the brand was founded and the circumstances surrounding it at the outset form a starting point; origin stories can be important in shaping the brand's image;
- Development and growth: the evolution of the brand over time, and the strength of its spread and expansion into new areas, or its winning of marketing gambles and product development... all these details show how they affected the brand's growth and development;
- Stages of change: the changes and transformations the brand has undergone over time, which may include changes in the brand's identity, marketing strategies, and audience interaction;

- Notable events: important events the economic institution has witnessed, such as the launch of major products, strategic partnerships, local, national, or international expansion, or the institution going through a crisis — all of which affect the brand's trajectory;
- Reputation record: how the brand has been received by the public and the market over time, and whether there were periods of acclaim or challenges to the brand's reputation;
- Evolution of the logo and visual identity: changes in the brand's logo or visual identity over time reflect changes in the perception of the brand and its response to shifting trends;
- Historical value: historical stories and narratives associated with the institution's brand may add cultural and emotional value to its experience with the public.

3.2.2. The Target Audience Dimension :

The brand's target audience refers to the categories and groups the brand aims to communicate with and whose needs and desires it seeks to satisfy. This dimension relates to understanding the people who constitute an important audience for the institution and how to interact with them effectively, through studying the target audience cognitively, emotionally, and behaviorally. This dimension also studies consumers' attitudes toward visual composition in integrated marketing communications and its impact on their purchasing decisions, given that there is a direct relationship between individuals' aesthetic inclination and the formation of positive attitudes toward the use of metaphor in marketing communications.

The target-audience dimension includes the following elements:

- Identifying target categories: in building their visual identity, economic institutions cannot, under any circumstances, dispense with knowledge of the groups concerned with the product they wish to market to them; for this reason, the fit between the institution and its audience must be studied to understand their inclinations and tastes, in order to determine the appropriate colors and typography for building the logo;
- Choosing appropriate communication means: choosing the channels and communication means that best reach the target audience, which may include social media, television advertisements, print advertisements, and email marketing.

3.2.3. The Competitive Dimension :

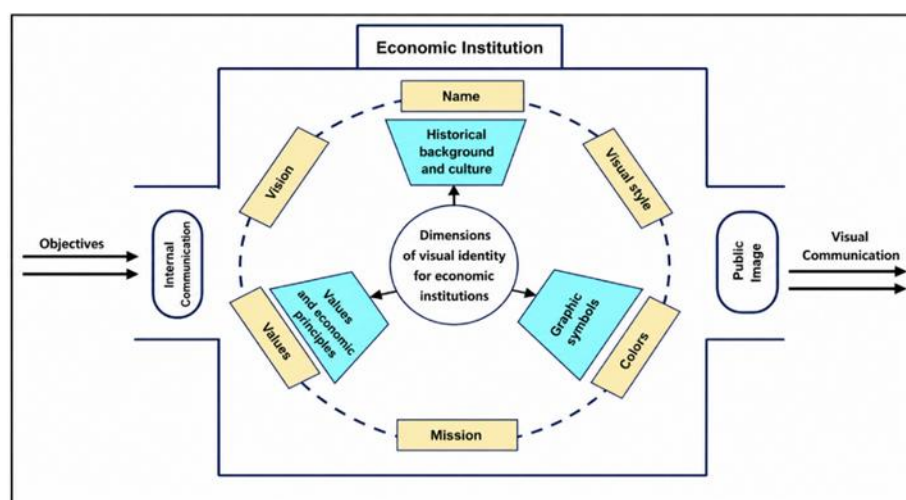
The competitive dimension of the visual identity of economic institutions is extremely vital, as it relates to how the institution distinguishes itself from its competitors through the design elements of the brand that form its visual identity, and aims to make the institution distinctive in the minds of the public and enhance its preference over competitors.

The main elements of the competitive dimension of visual identity include:

- Distinctiveness and uniqueness: designing a unique visual identity that makes the institution stand out among competitors and distinguishes it in the market;
- Creativity and innovation: using innovative and creative design elements to attract the audience's attention and create a distinctive experience;
- Consistency: ensuring balance and consistency among all elements of the visual identity, which enhances its recognizability and distinctiveness;

- Effective communication: designing expressive communication elements that convey the institution's message effectively and attractively;
- Emotional impact: building an emotional connection with the audience through visual identity, which enhances loyalty and preference;
- Customer experience: designing the visual identity in a way that reflects the institution's values and experience, positively affecting the customer experience;
- Visual representation of values: using colors, symbols, and images that express the institution's values and distinguish it from others;
- Influence on decision-making: using design elements to create a positive, distinctive impression in the audience's mind, thereby affecting the decision-making process.

Figure 1: *A model illustrating the impact of the dimensions of visual identity on the economic institution.*



Source: Prepared by the researcher.

3.3. The Information Security System :

In the age of the information revolution, it has become very easy to breach institutions' information networks, gain access to them, and learn the most precise secrets; those who infiltrate an information network may be mere amateurs with no specific goals, or professionals who leak the information they obtain to their counterparts in competing or hostile institutions, or they may even be the institution's own employees, whose goal is to find out the institution's position toward them or to obtain secrets with which they can bargain with the institution.

3.3.1. The Information Security System :

Terminologically, specialists have offered several definitions of the concept of information security, which generally agree in overall context with some slight differences; among these definitions we find the following:

It is defined as a science that examines the theories and strategies for providing protection to information from the risks that threaten it and from activities that attack it; from a technical angle, it is a

set of tools and procedures necessary to ensure the protection of information from internal and external dangers that prevent information from reaching unauthorized persons; and from a legal angle, information security represents a field of study and a set of measures aimed at protecting the confidentiality of information, the integrity of its content, and its availability, as well as combating activities that attack it or exploit its systems to commit crimes.

The U.S. Committee on National Security Systems (CNSS) defines it as "the protection of information and its critical elements, including the systems and devices that use and store this information" (Whitman, Mattord, 2021).

It is also defined as "all the policies, procedures, and technical tools used to protect information from all illegitimate forms of resource use, such as theft, alteration, modification, and intentional damage to information" (Karaz, 2021).

It is also defined as a state of security that is free of risks or that limits them — meaning protecting information from adversaries who wish to cause it harm, whether intentionally or unintentionally; for this reason, it is necessary to establish a set of multiple security layers consisting of the following elements (Singh, 2014):

- a-** Physical security: to protect the institution's physical elements or objects from unauthorized access and misuse;
- b-** Personnel security: to protect the individual or group of individuals authorized to access the institution's data and operations;
- c-** Operations security: to protect the details of an operation or a series of specific activities;
- d-** Communications security: to protect the institution's communication media, technology, and content;
- e-** Network security: to protect the institution's networks (the gatekeeper);
- f-** Information systems security: to protect information and its important elements, including systems and devices.

From these definitions, it can be inferred that, theoretically, an information security system is a strategic plan aimed at protecting the data and information owned by the institution, and controlling who can access it or dispose of it, by allowing only those who possess the qualifications and authorizations determined by the institution to do so.

From a technical point of view, Rúsbel Domínguez defines an Information Security Management System (ISMS) as a system that manages risk based on the methodologies of international rules and standards (ISO/IEC 27000); ISMS standards make it possible to measure threats and help detect vulnerabilities in organizations' information systems, and the implementation of these techniques enables managers to make better decisions. However, if an institution fails to manage information security, or if the integrity of its data is breached, negative effects will follow (Rúsbel, 2023).

Information security (Infosec) is also defined as a set of strategies for managing the processes, tools, and policies necessary to prevent, detect, document, and combat threats targeting digital and non-digital information. The responsibilities of information security include creating a set of processes that protect information assets, regardless of how the information is organized or whether it is being transmitted, processed, or stored (Yasar, 2016). A distinction can be made between digital and non-digital information as follows:

- Paper-based (non-digital) information security system: this term is used to describe a system that keeps information on paper rather than on a computer (Cambridge, 2023).

- Cybersecurity (digital) system: cybersecurity is the practice of protecting critical systems and sensitive information from digital attacks; cybersecurity measures are also known as information technology (IT) security, and are designed to combat threats targeting networked systems and applications, whether these threats originate from inside or outside the institution (Intro Cybersecurity, 2023).

Most researchers, bodies, and international institutions in the field of information security consider that the CIA triad — that is, the principles of an information security system — represents a set of very important requirements for such a system, namely (Taylor, 2008):

a- The principle of confidentiality of information: the property that prevents information from being made available or disclosed to unauthorized individuals, entities, or processes. Information is often applicable only to a limited number of individuals because of its nature or content, or because wider distribution would produce undesirable effects, including legal or financial penalties or embarrassment to one party or another. Restricting access to information to those who have a "need to know" is good practice based on the principle of confidentiality; controls that ensure confidentiality form a major part of the broader aspects of information-assurance management.

b- The principle of the integrity of information: the property of maintaining accuracy and completeness — information is useful only if it is complete and accurate. Preserving these aspects of information (its integrity) is often of critical importance, and ensuring that only certain persons have the appropriate authority to change, update, or delete information is another fundamental principle for ensuring information security.

c- The principle of availability: the property of being able to access and use information on demand by authorized persons or bodies; if information is not available when needed, it cannot be called information at all. The availability of information is one of the areas witnessing technological developments that have significantly increased the difficulties faced by information-assurance specialists compared with the past.

In the same context, and from a legislative perspective, the concept of information crimes — or so-called cybercrimes — emerged, addressing the substance of information security and the methods of confronting it through international charters, legislative laws, and decrees.

It can be affirmed that an information security system rests on fundamental concepts that can be summarized in the following points (Whitman, Mattord, 2021):

- Access: the user's ability to view information, holding legal authorization to access the system; without this legal authorization, this information cannot be accessed;
- Asset: the organizational resource being protected; an asset can be logical, such as the institution's website, software, or data, or it can be physical, such as a person, a computer system, or a device — information assets in particular are the focus of what security efforts try to protect;
- Attack: a deliberate or unintentional act that can harm, or otherwise endanger, information and the systems that support it; attacks can be active or passive, intentional or unintentional, direct or indirect;

- Control, protection, or countermeasure: mechanisms, policies, or security procedures that can successfully confront attacks, reduce risks, address vulnerabilities, and contribute to improving the institution's level of security;
- Exploit: a technique used to breach a system — the term can be a verb or a noun; threat agents may try to exploit a system or another information asset by using it illegally for personal gain, or an exploit can be a documented process undertaken to take advantage of a security vulnerability or exposure, whether inherent in the software or created by the attacker; exploits make use of existing software tools or purpose-built software components;
- State of exposure: in information security, exposure exists when a security vulnerability is known to the attacker;
- State of loss: when an information asset is exposed to harm or destruction;
- Risk: the probability of an undesired event occurring, such as a negative event or a loss;
- Subjects and objects of attack: a computer can be the object of an attack — for example, it can be breached by an entity and then used to attack other systems;
- Threat: any event or circumstance that is likely to adversely affect the institution's information system.

3.3.2. Sources of Information Security Threats :

According to researchers Howard and Benson, there are two sources (Hamed, 2019):

- Information security threats from natural disasters: such as floods, fires, and earthquakes.
- Human threats: such as intrusion, espionage, and hacking.

Other researchers have added a physical source of threat, such as power outages and network or software failures; nevertheless, most researchers agree that threats arising from human behavior most affect the success or failure of an organization's efforts to secure its business, services, systems, and information (Efthymia, 2014).

3.3.3. Technical Methods of Information Security Systems :

There are multiple means of protection against various threats, and an information security system relies on a set of tools and procedures, among which we find:

- a-** Electronic encryption: a mathematical process (an algorithmic equation) through which the text to be sent is converted into codes and signals that cannot be understood except after decryption;
- b-** Hash-function applications: a set of applications aimed at achieving the integrity of information; also an algorithm that works to ensure the secure exchange of information;
- c-** Electronic signature: uses a particular method to verify the identity of the party to a transaction; the most prominent forms of electronic signature are the electronic fingerprint, iris scan, and electronic signature;
- d-** Password: without a password, no unauthorized person can access the information network; it is one of the simplest types of protection;
- e-** Firewall: a program used to protect networks and servers from intruders and hackers; it is an IT security solution through which access-control policies are set to determine who is authorized to enter and who is not;

f- Network address translation: this technique relies on giving each device connected to the network a distinctive number that differs from other devices; the organization assigns these numbers, and they are not recognized except through it;

g- Automatic updating: one of the most important means of information protection, because the process of building these systems is extremely complex, so any program needs to be updated to increase its level of security;

h- Backup storage: copying contents and information and keeping these copies in a secure place, so that they can be retrieved when needed;

i- Data wiping: most users believe that simply deleting a file means it is permanently lost, even if it is deleted from the recycle bin — but this is not true; deleting a file from a storage unit deletes the pointer indicating it, not the file itself, which is why it must be wiped. There are three types: wiping the file upon deletion, wiping free space on the storage unit, and using the swap file, which is a file specific to the operating system.

3.4. Challenges Faced by Economic Companies Regarding the Impersonation of Their Visual Identity, and Methods of Confronting Them :

3.4.1. The Increase in Cases of Imitation and Counterfeiting :

Table 2: *Cases of product imitation and trademark impersonation among a number of global economic institutions.*

Institution	Case / Information	Type of Visual-Identity Impersonation	Targeted Element	Channel	Detection / Control Mechanism	Protection / Countermeasure Mechanism	Legal Action	Communicative Impact	Degree of Relevance to Information Security	Source
Apple	90% of Apple chargers on Amazon found to be counterfeit	Brand and product imitation	Logo, design, and packaging	Amazon	Investigation of products and sellers	Brand protection and market monitoring	Federal lawsuit	Threat to consumer trust	High	Forbes

	IP- rights director 's testimo ny before Congre ss	Brand imitati on (genera l context)	Apple identit y and access ories	Legisl ative body (U.S. Congr ess)	Investi gations and reports	IP protecti on	None / no direct legal action (advis ory testim ony only)	Protecti ng trust and safety	High	House Energy & Comme rce Commit tee
Sam sung	Delhi factory assembl ing counter feit phones; 512 devices seized	Brand and identity impers onation	Galax y, IMEI labels	Local marke t (India)	Police raid	Seizure of product s and investig ation	Arrest of those involv ed (FIR 1483/2 025)	Protecti ng brand trust	High	Beebom
	Counter feit Galaxy phones on Facebo ok Market place	Visual identity impers onation	Galax y name and brand	Faceb ook Mark etplac e	Verific ation and reports	Official docume nted consum er warning	None / no direct legal action	Protecti ng consum er trust	High	Sammy Fans
Cisc o	Smuggl ing of counter feit network ing equipm ent worth	Brand impers onation	Cisco logo and netwo rking equip ment	Intern ationa l marke t	Federa l investi gations	Supply- chain monitor ing	Federa l indict ment	Protecti ng reputati on and trust	Very high	U.S. DOJ

	over \$1 billion									
	Global brand-protection management (+50 staff, 15 countries)	Not applicable (countermeasure mechanism, not an impersonation incident)	Brand and products	Global	Intelligence and investigations	Brand Protection and anti-counterfeiting technologies	None / no single legal action (standing institutional activity)	Protecting brand and trust	Very high	Authentication Brand News
HP	Seizure of 2.6 million counterfeit cartridges (H1 2022)	Brand and product imitation	HP logo and packaging	Mark etplaces and Amazon	Investigation and takedown	Anti-counterfeiting	Removal and seizure actions (no specific lawsuits mentioned)	Protecting trust in products	High	Actionable Intelligence
	Seizure of 460,000 HP/Samsung cartridges in the UAE	Brand imitation	Brand and packaging	Market (UAE)	Customs inspection	Anti-counterfeiting	Customs confiscation	Protecting consumer trust	Medium	Gulf News
Intel	Counterfeit Core i7-	Brand impersonation	Intel and	Market	Detection of counterfeit	Authenticity	None / no document	Protecting technical	Medium	The Register

	920 process ors (2010)		Core i7		rf e it p ro d u c t s	ver i f i c a t i o n	ent e d l e g a l a c t i o n	a l c r e d i b i l i t y		
	Counter feit process ors hard to distingu ish (2020)	Identit y impers onation	Brand and proce ssor specif icatio ns	Mark et (Chin a)	Inspect ion and verific ation	Authent icity- verificat ion technol ogies	None / no docum ented legal action	Protecti ng trust in Intel	High	Tom's Hardwa re
LG	Seizure of 4,449 counter feit LG/AS US phones (over \$941,00 0)	Brand imitati on	LG logo and phone desig n	Mark et (Unit ed States)	U.S. Custo ms	Custom s inspecti on	Custo ms confis cation	Protecti ng brand image	Medi um	U.S. CBP
Sony	Smuggl ing of counter feit video cameras bearing the Sony brand	Brand impers onation	Sony logo and camer a identit y	Intern ationa l trade	Custo ms investi gation (ICE/ HSI)	Verifica tion and monitor ing	Crimi nal charge s filed	Protecti ng brand reputati on	Medi um	U.S. ICE
Huawei	Counter feit phones and access ories reachin	Brand impers onation	Logo, phone , and access ories	Stores and platfo rms	Investi gation and reports	Brand Protecti on	None / single docum ented legal action	Protecti ng consum er trust	High	Huawei (official)

	g physica l stores									
Xiao mi	Seizure of over 2,000 counter feit product s in Delhi	Brand imitati on	Xiao mi produ cts and logo	Mark et (India)	Police raid	Anti- counterf eiting (with police escort)	Confis cation	Protecti ng consum er and brand	Medi um	TechRa dar
	Decline in genuine power- bank sales due to counter feiting	Produc t imitati on	Produ ct and brand	Gener al marke t	Compa rison of sales figures	No specific counter measure mechan ism mention ed	None / no docum ented legal action	Econo mic losses and impact on trust	Medi um	Bloomb erg
	Chenna i and Bangal ore seizures (3.33 million rupees)	Brand imitati on	Produ cts and brand	Mark et (India)	Police inspect ion	Anti- counterf eiting	Confis cation	Protecti ng brand trust	Medi um	The Tribune India
Dell	Compla ints of counter feit batterie s/charg ers on Amazo n under the Dell name	Brand impers onation	Dell name and produ ct	Amaz on	User reports	Digital- channel monitor ing	None / docum ented forum compl aints only	Protecti ng custom er trust	High	Dell Commu nity

Philips	Seizure of 236 counterfeit LED units in China	Brand imitation	Philips logo and product design	Mark et (China)	Inspection and raid	Authenticity check (company representative present)	Administrative confiscation	Protecting credibility	Medium	LEDinside
Panasonic	Counterfeit products and entirely fake products	Brand impersonation	Panasonic logo and name	Mark et	Field verification	Awareness campaign + customs training	None / single documented legal action	Protecting trust and safety	Medium	Panasonic
	IP-rights registration in 41 countries	Not applicable (preventive mechanism, not an impersonation incident)	Intellectual property and brand	Customs, worldwide	Registration and monitoring systems	Rights registration with customs (this is the protection mechanism itself)	Official customs cooperation	Protecting corporate identity	High	Panasonic Holdings
Amazon	\$1.2 billion investment; seizure of 7 million counterfeit products (2023)	Not applicable (platform countermeasure system, not a type of	Brands, images, and product names	Amazon platform	AI-based detection systems	Operational investment + dedicated team (15,000 staff)	Removal of listings and action against sellers	Protecting trust of platform users	Very high	Retail Dive (citing Amazon)

		impersonation)								
	About 15 million counterfeit products (2025 report)	Not applicable (system performance indicator, not a type of impersonation)	Brands and products	Amazon platform	Detection systems (SENTRIX)	AI and data analysis	Removal of products	Protecting trust in the platform	Very high	WorldE F
Bosch	Seizure of 152 million counterfeit goods in the EU (2023)	Brand imitation (general sector context, not specific to Bosch alone)	Bosch logo and products	European market	Customs seizure operations	Market monitoring	Confiscation (at EU level)	Protecting reputation	Medium	Bosch Press
	Cooperation with KPDN and PDRM (Malaysia)	Brand imitation	Brand and products	Malaysian market	Investigations and raids	Supply-chain monitoring	Confiscation in cooperation with authorities	Protecting brand trust	Medium	Bosch Malaysia
Google	Official page for reporting	Not applicable	Google and	Internet and	User reports	Reporting and verification	None / single document	Protecting user trust	High	Google Support

	g counter feit Nest/St ore product s	(preven tive reporti ng tool)	Nest logo	marke t		ion system (label + QR)	ented legal action			
Can on	Seizure of 1,775 counter feit cartridg es in India (May 2026)	Brand imitati on	Cano n logo and packa ging	Mark et (India)	Raid	Authent icity check	Arrest s (4 indivi duals)	Protecti ng brand trust	Medi um	The Recycle r
Eps on	Joint lawsuit with Amazo n against sellers of counter feit ink bottles	Brand imitati on	Brand and packa ging	E- comm erce	Tracki ng of sellers	Platfor m monitor ing	Federa l lawsui t	Protecti ng trust in product s	High	Epson (news.e pson.co m)
	\$7.2 million damage s award for Epson and Amazo n	Brand imitati on	Brand and produ ct	E- comm erce	Legal investi gation	Product and seller tracking	Enforc eable federal court judgm ent	Deterri ng counter feiting and protecti ng reputati on	High	Law360
Brot her	Seizure of 6,200 counter	Brand imitati on	Broth er logo	Mark et	Police inspect ion	Authent icity check	Distrib utor	Protecti ng	Medi um	Gulf News

	feit ink cartridges in Ajman/ Dubai		and packa ging	(UAE)			detai ned	brand trust		
Daikin	Rising counter feiting of Daikin product s in Asia	Brand impers onation	Brand and desig n	Mark ets and e- comm erce	Market /websit e monito ring + custom s monito ring	Product registrat ion with customs	None / single docum ented legal action	Protecti ng brand identity and custom er trust	High	Daikin

Source: Prepared by the researcher.

The documented cases reveal the breadth of the phenomenon of product and trademark counterfeiting among a large number of global economic institutions; the phenomenon has included brands such as Apple, Samsung, Cisco, HP, Intel, LG, Sony, Huawei, and Xiaomi, ranging from the imitation of products and accessories, to the copying of marks and identifying elements, to the forgery of identification numbers and components. For example, the Apple case revealed the widespread presence of counterfeit accessories on Amazon, while Indian authorities documented a factory assembling counterfeit Samsung Galaxy phones, seizing hundreds of devices, motherboards, and forged IMEI labels. The Cisco case likewise revealed a network smuggling counterfeit networking equipment with a retail value exceeding one billion dollars. These cases confirm that counterfeiting is no longer a limited or individual activity, but has become an organized, cross-border phenomenon targeting economically valuable products and globally present trademarks.

The data also show that counterfeiting extends to various components of visual identity, including accessories, printing supplies, electrical tools, and lighting products. HP announced the seizure of about 2.6 million counterfeit ink cartridges during the first half of 2022, while other documented cases linked to Philips, Panasonic, Canon, Epson, and Daikin involved action against counterfeit products or supplies. The Bosch case also reveals the large scale of the phenomenon, with 152 million counterfeit goods seized in the European Union during 2023, a 77% increase over the previous year. Counterfeiting is not confined to traditional markets but extends into the digital environment; Google has created an official channel for reporting counterfeit products, while Amazon has taken extensive measures to combat the phenomenon, including large investments, the deployment of thousands of employees, and the seizure of millions of counterfeit products. This data shows that the spread of e-commerce and the multiplicity of distribution channels have contributed to widening the scope of the problem and complicating the process of verifying the authenticity of products.

From a communicative perspective, the danger of this phenomenon lies in the fact that the counterfeit product does not merely copy the physical function of the product, but exploits the institution's name, brand, and visual and identifying elements to produce a false impression of authenticity for the consumer. This danger increases when counterfeit products become difficult to distinguish from the original, as the data indicated in the Intel case, or when the products reach physical stores and electronic platforms, as in the Huawei case and others. Institutions have therefore become required to go beyond traditional anti-counterfeiting methods toward an integrated system that combines legal and customs protection, digital monitoring, authenticity-verification mechanisms, and reporting channels and cooperation with the relevant platforms and authorities. Accordingly, the increase in counterfeiting cases reveals the transformation of the problem from mere product imitation into the impersonation of the institution's commercial identity, which makes the activation of information security systems and digital protection technologies one of the important entry points for limiting visual identity impersonation and protecting stakeholders' trust in the brand.

3.4.2. Challenges of E-Commerce in Visual Identity Impersonation :

Table 3: *Challenges of e-commerce in visual identity impersonation.*

Institution	Documented Information	Type of Action / Source
Apple	The most impersonated brand worldwide on fraudulent websites, according to actual web analysis; and exact copies of login pages used to steal authentication credentials	Analytical report (McAfee) + official support page
Samsung	Official statement (Hong Kong) denying any connection to fraudulent websites; and a warning about counterfeit Galaxy phones on Facebook Marketplace	Official statement + support page
Cisco	Criminal referral to the Shenzhen police leading to the seizure of more than 500 counterfeit units, 3,100 forged labels, and 27,000 booklets distributed via electronic platforms	Official blog (Cisco Blogs)
HP	Removal of more than 10,000 counterfeit listings/pages and seizure of 670,000 counterfeit products (Q1 2026); a lawsuit with Amazon against "HP Supply LLC"	Official statement + lawsuit
LG	Proactive acquisition of the domains "LG"/"LGbrand"/"BEST"; a logo and animated hologram provided electronically to authorized distributors	Official statement (Korean)
Sony	Actual lawsuits filed in Illinois against sellers on Amazon/eBay/Temu/Walmart, with damage claims of up to \$2 million per violation	Documented lawsuits

Xiaomi	Detection and takedown of a fake website (mi-home.in) that exploited the COVID-19 pandemic, with an official report filed to cybercrime authorities	Documented media report
Panasonic	Periodic monitoring of about 1,000 e-marketplaces in 100 countries; 68 reported infringement cases on Taobao; a raid in Malaysia targeting products advertised on Shopee/Lazada	Official statement (Panasonic Holdings + Panasonic Malaysia)
Philips	Counterfeit toothbrushes on the Temu platform remained listed until hundreds of purchases had accumulated before removal	Independent research report (ITIF)
Amazon	The AI-based SENTRIX system predicted a bad-actor attack and blocked the listings eight days before the trademark owner filed a report	Official report (aboutamazon.com)
Broadcom	Official "Counterfeit & Gray Market Awareness Statement" warning against unauthorized online sellers who run professional-looking websites lacking genuine contact information and selling products at suspiciously low prices	Official page (broadcom.com)
Canon	An official page (Canon Europe) titled "Warning Signs of a Fraudulent Website" to raise consumer awareness; and a journalistic investigation based on nearly 24 official complaints filed with the U.S. Federal Trade Commission (FTC) regarding fake customer-service websites impersonating Canon	Official page (Canon Europe) + journalistic investigation (citing FTC complaints)

Source: Prepared by the researcher.

The table reveals that e-commerce has created a sophisticated environment for the impersonation of institutions' visual identity, as impersonation is no longer limited to imitating the physical product but has extended to websites, sales pages, digital accounts, logos, images, packaging, and the brand's identifying elements. The Apple case clearly demonstrates this through fraudulent websites that impersonate the brand's online presence, including the copying of login pages, while the Samsung case reveals fraudulent websites impersonating the institution's affiliation, alongside the display of counterfeit Galaxy phones via Facebook Marketplace. The Xiaomi case shows a fake website that exploited the brand's name to target buyers, while the Canon case points to customer-service websites impersonating the institution. These cases confirm that the digital space now allows the reproduction of an institution's visual identity within digital interfaces that appear to the user as though they belong to the original brand, which increases the difficulty of verifying the true source of the party the consumer is dealing with.

The table also shows that the multiplicity and breadth of e-commerce platforms constitute an additional challenge to the protection of visual identity. Cases of imitation or impersonation have been linked to multiple platforms, including Amazon, eBay, Temu, Walmart, Facebook Marketplace, Shopee,

Lazada, and Taobao. The Cisco case appears in the seizure of counterfeit units and forged identifying materials linked to sales via electronic platforms, while the Sony case reveals lawsuits against sellers on several electronic platforms, and Panasonic documents its reliance on monitoring a large number of e-marketplaces across multiple countries. The Philips case also reveals the continued display of counterfeit products on Temu until purchases had accumulated before their removal. This indicates that the problem is not linked to a single platform, but to the multiplicity of product-display points, the diversity of sellers, and the speed with which commercial content moves between them — which makes the detection and follow-up of impersonation a continuous process rather than an action confined to a single channel.

On the other hand, the table shows that institutions have begun developing direct digital responses to confront these challenges. HP has relied on extensive removal of counterfeit listings and products, while Amazon uses an AI-based system to predict malicious activity and block certain listings before they are reported by trademark owners. LG resorts to proactive measures related to domain names, and to visual verification elements for authorized distributors, while Panasonic relies on periodic monitoring of e-marketplaces, and Cisco uses criminal proceedings to protect its brand from counterfeit products. These cases reveal that confronting visual identity impersonation in e-commerce now requires moving from reacting after impersonation occurs to early monitoring, detection, and digital intervention, especially given the ability of electronic platforms to reproduce infringing content and spread it rapidly.

Accordingly, it can be concluded that the fundamental challenge posed by e-commerce in the field of visual identity impersonation lies in the combination of the ease of digitally reproducing the institution's identity, the multiplicity of platforms and sellers, the breadth of the cross-border market, and the difficulty of instant authenticity verification. The cases presented in the table reveal that impersonation takes multiple forms, beginning with the imitation of products and marks and extending to the creation of websites, pages, and accounts that suggest an official relationship with the institution. Consequently, protecting visual identity in the digital marketplace does not stop at registering the trademark or protecting the product design, but requires the institution to monitor the brand's own digital presence and detect illegitimate uses of its visual and identifying elements, together with speed of reporting, removal, and appropriate action. This is what makes the digital environment an increasing challenge for institutions seeking to preserve the authenticity of their identity and the public's ability to distinguish between their official presence and an impersonating presence.

3.4.3. Enhancing Customer and Consumer Awareness

Table 4: *Enhancing customer and consumer awareness.*

Company	Documented Awareness Initiative	Source
Samsung	Official awareness page (Australia) with precise comparison images between genuine and counterfeit	https://ushl.samsung.com/au/support/newsalert/117041

	AKG headphones and Icon X devices	
Cisco	"Education and Awareness" as an official pillar among six announced strategic pillars at Cisco Live 2023; an "anti-counterfeit identification platform" to educate partners and customers	https://www.ciscolive.com/... (Cisco Live materials); https://www.hi-network.com/3-key-steps-to-protect-your-network-from-counterfeit-cisco-products.html
Huawei	Official page with five detailed tips for recognizing the genuine product (buying from authorized sellers, pricing, the security seal, the QR code)	https://consumer.huawei.com/en/legal/brand-protection/how-to-avoid-counterfeit-goods/
Xiaomi	Official press release advising consumers to verify the "security code" via the official website following the Delhi seizure incident	https://www.newsbytesapp.com/news/business/how-to-spot-fake-and-counterfeit-xiaomi-products/story
LG	Official awareness campaign called "I Love Genuine" (Kenya) with a mobile-phone verification platform for products purchased since 2012	https://gadgets-africa.com/2020/04/30/lg-products-verification-service-platform/
Sony	Official support page (Asia) with precise visual comparisons of logos and holograms, and warnings about the	https://www.sony-asia.com/electronics/support/articles/00200902

	dangers of counterfeit batteries	
Philips	A comprehensive official awareness campaign called "Buy Original" (Ghana and West Africa) with a dedicated SMS line for verifying lighting products	https://www.modernghana.com/news/624411/philips-launches-buy-original-campaign-to-highlight-the-ex.html
Panasonic	(Previously documented in section 3.4.1): training of customs officers in Thailand and Vietnam + an awareness video about a counterfeit-iron fire incident	https://holdings.panasonic/global/corporate/about/intellectual-property/brand-protection.html
Amazon	The official Transparency program (available in 10 countries) with a scanning app for verifying authenticity, along with testimonials from brands enrolled in it	https://www.aboutamazon.com/news/innovation-at-amazon/amazon-transparency-protects-more-than-10-000-brands
Bosch	Origify technology for verification via a smartphone app, without the need for additional labels or codes	https://www.bosch-origify.com/
Google	Official page with actual comparison images between genuine and counterfeit Chromecast and Pixel devices + a QR-	https://support.google.com/store/answer/9096512?hl=en

	scanning system for Pixel 6 and later phones	
Microsoft	A full official "How To Tell" portal with multiple sections (COA label, Xbox hologram, safe-purchasing tips)	https://www.microsoft.com/en-us/howtotell/default
Canon	An official survey study (Anti-Counterfeit Study) showing that 71% of American consumers became less inclined to purchase counterfeit products after awareness efforts	https://www.bgr.com/general/how-to-spot-fake-electronic-devices/
Epson	Development of a new thermal and optical hologram label (Philippines) to raise awareness of the difference between genuine and counterfeit ink	https://www.dotdailydose.net/2022/04/19/epson-fake-printer-inks/
Daikin	An official step-by-step guide (Malaysia) for identifying genuine parts via the hologram and the 8-digit security code	https://www.daikin.com.my/tips/how-to-identify-genuine-daikin-parts-a-step-by-step-guide/

Source: Prepared by the researcher.

The table shows that enhancing customer and consumer awareness has become one of the fundamental components in confronting visual identity impersonation in the digital environment, as economic institutions move toward providing consumers with tools and knowledge that enable them to distinguish between the original and the counterfeit product and to verify its source before purchase. This awareness takes multiple forms, including direct visual comparison, as with Samsung, Sony, and Google, where images or indicators are provided to help the consumer notice differences in logos, holograms, packaging, and the product's visual elements. Huawei likewise relies on providing practical guidance

related to the source of purchase, the price, the security seal, and the QR code, making the verification process part of the consumer's own behavior.

The table also reveals another trend: a shift from traditional awareness to digital authenticity verification. Xiaomi has relied on verifying the security code via its official website, while LG provides a mobile-phone verification platform, and Amazon, through its Transparency program, allows scanning codes to verify products covered by the program. Bosch likewise offers its Origify technology, which enables verification using a smartphone, while Daikin uses holograms and a security code as part of the process of identifying genuine parts. This means that the consumer is no longer merely a recipient of warnings about counterfeit products, but has become a participating party in the authentication process through digital tools linked to visual identity or to unique product characteristics.

The table also shows the diversity of awareness channels among official pages, guidance manuals, media campaigns, phone-based verification tools, and digital scanning technologies. This is evident in LG's "I Love Genuine" initiative, Philips' "Buy Original," Microsoft's "How To Tell" portal, and the awareness materials provided by Panasonic and Cisco. This diversity reflects institutions' recognition that protecting visual identity is not achieved solely through legal measures or the monitoring of electronic markets, but also requires raising the consumer's ability to recognize the original brand and detect manifestations of impersonation.

Accordingly, the cases presented in the table reveal that consumer awareness represents a link between protecting the institution's visual identity and reducing the chances of successful impersonation in e-commerce. The clearer the indicators available to the consumer for verifying authenticity — whether through visual marks, security codes, or digital verification tools — the more capable the consumer becomes of making an informed purchasing decision. Awareness in this context is therefore not limited to providing warning information, but is transformed into a participatory preventive mechanism that makes the customer part of the system protecting the institution's visual identity.

3.4.4. Application of Advanced Detection Technologies :

The data presented in the table reveal that the development of technologies for detecting visual identity impersonation is no longer based merely on adding a security mark to the product, but has come to move toward building a verifiable identity for the product and linking it to the original product and to the institution's digital system. This shift becomes clear when comparing technologies that rely on the visual characteristics of the packaging with technologies that use digital codes or unique identifiers, and then with technologies that make verification linked to the physical structure of the product itself. Thus, the difference between institutions lies not only in the type of technology used, but in the level at which the identity being verified exists: is it on the packaging? Inside the institution's database? Inside the device itself? Or in the product's physical characteristics?

A group of technologies found in the studied cases make visual identity the entry point into the detection process. The security labels and holograms used in HP, Sony, Daikin, and Microsoft products rely on visual characteristics that are difficult to imitate by traditional means, such as a change in appearance depending on the viewing angle, or the presence of multiple holographic elements. However, the importance of these technologies does not lie merely in their being advanced visual elements, but in the fact that they transform visual identity from a mere identifying logo into a security mark carrying the

function of proving authenticity. In the case of HP, for example, inspection does not stop at noticing the visual changes in the label, but can move from visual inspection to digital scanning of a QR code, combining visual and digital evidence. Daikin, for its part, combines hologram characteristics, a security code, and a QR code in a single verification process. Thus, the visual mark here is no longer the final goal of detection, but has become part of a multi-stage verification chain.

This reveals a fundamental problem facing institutions in the digital environment: the ability to copy a visual identity no longer necessarily means the ability to prove authenticity. The logo, the image, the color, and the packaging design are all elements that can be digitally reproduced; indeed, some counterfeit products can be so visually well-crafted that judging them by eye alone becomes difficult. A growing trend has therefore emerged toward adding an element that cannot be verified visually alone, but requires reference back to an official system. This is evident in Huawei, Xiaomi, and Google, where the authentication process is not limited to seeing the mark or seal, but relies on entering or scanning an identifier linked to the product and then referring back to the institution's system to verify it. Detection thus shifts from the logic of visual resemblance to the logic of digital matching.

This shift takes on particular importance in e-commerce, because the consumer often makes a decision based on the product's image, name, logo, and the seller's page before being able to physically inspect the product. Digital verification therefore provides the institution with a mechanism for intervening at the very moment the visual identity is vulnerable to exploitation on the electronic platform. A product bearing an original name and logo does not become genuine merely because its image matches that of the official product; rather, it must have a verifiable identity within the official system. From this angle, QR technologies, the serial number, the IMEI, and security codes become tools for transforming visual identity from a copyable image into a digital, authenticatable identity.

Amazon Transparency provides an important example of this shift, because authentication here does not occur only after the product reaches the consumer, but can be part of the product's journey within the e-commerce system. The system is based on encoding registered units with unique codes, and these codes can be used to verify the product at various stages, including verification by the consumer. Thus, the technology does not protect the logo or packaging merely as a visual appearance, but links the physical unit of the product to a digital record that can be referred back to. This changes the nature of the relationship among the institution, the platform, and the consumer: the consumer no longer merely compares the product visually, and the platform no longer merely displays the seller's data; rather, the unique code becomes the link between the actual product and the authentication data.

The degree of technical complexity increases when identity moves from the packaging to inside the product itself. Cisco represents, in this context, a case different from label technologies; it uses SUDI in some of its devices, a digital identity linked to the device and backed by a physical trust element inside it. Here, verification does not depend on the consumer's ability to detect a visual difference in the packaging, but on the ability to verify the identity of the device itself. This type of authentication is more relevant to technical products intended for professional use, because the fundamental question is not only "does the device bear the Cisco mark?" but rather "does the device about to be introduced into the network possess the digital identity that the original device is supposed to have?" Here, digital identity becomes part of the technical structure of the product, rather than a mere external attachment to it.

Bosch Origify offers another level of this development; instead of adding a label or code to the product, the technology relies on the fine natural characteristics of its surface as a means of recognition. The idea is based on recording these characteristics and converting them into a digital identity that can later be used for verification via a smartphone. The technical value of this model lies in the fact that the authentication element is not something separate from the product that can be removed or reprinted, but is linked to physical characteristics present in the product itself. Origify therefore reveals an important shift from protecting the mark found on the product to proving the identity of the product that bears the mark.

When comparing these levels, it becomes clear that the studied detection technologies differ in their degree of reliance on an external, reproducible element. The label and the hologram represent an important layer of protection, but they remain elements that a counterfeiter can attempt to reproduce. When a QR code or an online-verifiable security code is added to them, the counterfeiting process becomes more complex, because the counterfeiter needs not only to copy the appearance, but to produce an identifier that yields a correct result in the institution's system. When authentication becomes linked to the device's identity, as with SUDI, or to its natural physical characteristics, as with Origify, the scope for counterfeiting shifts from copying the appearance to copying an identity that is difficult to separate from the original product.

From here one can understand why technologies differ between product sectors. Institutions dealing with widely distributed consumer products, especially printing supplies and spare parts, find in security labels and holograms a practical means allowing the consumer or distributor to conduct a quick check. In contrast, electronic devices and networking equipment require deeper levels of authentication, because the value and function of the product do not allow reliance on external appearance alone. Hence Cisco has a digital identity linked to the device, while Bosch offers a model based on the product's physical characteristics. This does not mean that one level cancels out the other, but that the nature of the product determines the most appropriate position for placing the verification mechanism.

The studied cases also reveal a clear shift from passive detection to interactive detection. Passive detection means the consumer looks at the packaging and tries to judge its authenticity based on color, logo, print quality, or hologram. Interactive detection, by contrast, requires an action from the user, such as scanning a QR code, entering a security code, using the serial number or IMEI, or photographing the product to verify it. This shift is important because it makes the authentication process digitally documentable, and reduces reliance on personal visual impression. The consumer thereby becomes part of the verification process rather than a mere recipient of a brand that may be counterfeited.

In the same context, the cases reveal the importance of multiple layers of protection rather than reliance on a single technology. The presence of a hologram alone may not be sufficient, and the presence of a QR code alone does not necessarily guarantee the safety of the product if the code is copyable or reusable. Some systems therefore tend to combine two or more indicators: a visual characteristic, a digital code, a unique identifier, and a central database. The more the authentication process moves from mere recognition of shape to verifying the relationship among the mark, the product, the code, and the database, the more difficult identity impersonation becomes.

From the perspective of this study's subject, this finding carries a fundamental implication: technology does not protect visual identity only by preventing the imitation of its shape, but by linking that shape to another element that can be verified and that the impersonator cannot easily reproduce. The logo can be copied, the product image can be copied, and even the packaging can be imitated; but when the visual appearance is linked to a unique code in a database, or to a device identifier, or to recorded physical characteristics of the product, visual identity is transformed from a reproducible communicative element into a multi-layered, documented identity.

Accordingly, the technical development seen in the studied cases does not appear to be a mere transition from an old hologram to a newer QR code, but rather a deeper shift in the concept of identity protection: from protecting the mark as an appearance, to protecting the relationship among the mark, the product, and its source. It is this relationship that gives advanced detection technologies their value in combating impersonation, because the ultimate goal is not only to detect that the institution's logo has been used without permission, but to prove that the entity bearing that logo is indeed the product, account, or channel linked to the original institution.

Accordingly, an overall reading of the cases does not lead to viewing QR codes, holograms, IMEI, SUDI, or physical fingerprinting as competing technologies, but rather reveals a gradation in the depth of authentication. The process begins with the visual mark the user can notice, then moves to the security mark that is difficult to imitate, then to the digital identifier that can be verified via a database, and finally to an identity linked to the product's structure or its physical characteristics. The higher the level of authentication rises, the more the chances of success for impersonation based on reproducing the appearance alone decline. This is what makes the trend toward multi-layered authentication one of the most prominent features of the transformation in the protection of visual identity within the digital environment and e-commerce.

4. Conclusion :

The continuous transformation and rapid technological progress of our current era demonstrate the importance of activating an information security system as a fundamental measure for combating visual identity impersonation within economic institutions. Through the implementation of advanced, technology-based strategies, institutions can protect their reputation and quality, and ensure that their products and services remain safe from counterfeiting and imitation.

This study shows that the activation of an information security system involves a set of integrated measures, including the application of advanced detection technologies to identify subtle differences between original and counterfeit products. It also includes the application of a continuous monitoring and follow-up system for unusual and suspicious activities, which contributes to identifying any unusual pattern that could indicate identity impersonation. In addition, enhancing the security of data and communications requires the implementation of strong encryption and protection techniques for sensitive and important data.

The application of these measures contributes to building a fair and secure business environment that enhances the sustainable development of economic institutions. In addition to protecting consumers and customers from counterfeiting and impersonation, these measures contribute to enhancing trust in the market and enhancing institutions' reputation. Furthermore, combating visual identity impersonation

through an information security system achieves economic and social benefits, including enhancing competitiveness, stimulating innovation, and improving the quality of services and products.

Activating an information security system to combat visual identity impersonation represents a key step toward achieving a sustainable and trustworthy business environment in the age of technology and digitization. Through adopting these measures and integrating them effectively into institutions' strategies, comprehensive protection of visual identity and quality can be achieved, and their excellent reputation preserved in a market full of challenges and opportunities.

References :

- 1) Adebayo, O. P., Kehinde, O. J., Ogunnaike, O. O., Olaoye, O. P., & Adesanya, O. D. (2019). Corporate brand identity and service quality in higher education management. *Polish Journal of Management Studies*, 20(2), 45–59. DOI: <https://doi.org/10.17512/pjms.2019.20.2.04> .
- 2) Agarwal, S., & Vasek, M. (2026). Examining newly registered phishing domains at scale. *Journal of Cybersecurity*, 12(1), tyag020. DOI: <https://doi.org/10.1093/cybsec/tyag020> .
- 3) Al-Laban, S. D. (2000). *Communication technology: Risks, challenges, and social impacts*. Cairo, Egypt: Al-Dar Al-Masriya Al-Lubnaniya.
- 4) Taylor, A. (2008). *Information Security Management Principles*. Scotland: The British Computer Society.
- 5) Cambridge (2023). Meaning of paper-based. <https://dictionary.cambridge.org/dictionary/english/paper-based>. (17/08/2023).
- 6) Coman, C., Bularca, M. C., & Repanovici, A. (2021). Constructing and communicating the visual identity of a university. Case study: Visual identity of Transilvania University of Brasov. *Sustainability*, 13(13), Article 7145. DOI: <https://doi.org/10.3390/su13137145> .
- 7) CompaniesMarketCap. (24/08/2026). Largest electronics companies by market cap. 24/08/2026, 21:13. <https://companiesmarketcap.com/electronics/largest-companies-by-market-cap/> .
- 8) Cuntz, A., & Qian, Y. (2021). The Impacts of Counterfeiting on Corporate Investment. WIPO Economic Research Working Paper No. 67, World Intellectual Property Organization – Economics and Statistics Division. DOI: <https://doi.org/10.34667/tind.44630> .
- 9) Dorais, L.-J. (2004). La construction de l'identité. Dans D. Deshaies & D. Vincent (Éds.), *Discours et constructions identitaires* (p. 1–11). Québec, Canada: Presses de l'Université Laval. <https://www.erudit.org/en/books/culture-francaise-damerique/discours-constructions-identitaires/000660co/> .
- 10) Fathiya Hamed Salim Al Izki. (2019). Exploring the organisational, social and cultural factors influencing those employee attitudes and behaviours that impact the implementation of an information security culture within Omani organisations. [Doctoral thesis, University of Strathclyde].
- 11) Gregersen, M. K., & Johansen, T. S. (2022). Organizational-level visual identity: An integrative literature review. *Corporate Communications: An International Journal*, 27(3), 441–456. DOI: <https://doi.org/10.1108/CCIJ-06-2021-0068> .
- 12) International Trademark Association (INTA). (2023). *Anticounterfeiting Benchmarking Report – Executive Summary*. New York: International Trademark Association. <https://www.inta.org/wp->

[content/uploads/public-files/perspectives/industry-research/INTA-2023-Anticounterfeiting-Benchmarking-Report-Executive-Summary-05042023.pdf](#) .

- 13)** IntroCybersecurity. (2023). https://www.romanianunitedfund.org/intro_cybersecurity . (17/08/2023).
- 14)** Johansen, T. S., & Gregersen, M. K. (2024). The Authenticity of Organizational-Level Visual Identity in the Context of Strategic Communication. *International Journal of Strategic Communication*, 404–423. DOI: <https://doi.org/10.1080/1553118X.2024.2352114> .
- 15)** Karaz, S. E. (2021). The role of IT governance in enhancing information security. *Tishreen University Journal for Research and Scientific Studies – Economic and Legal Sciences Series*, 43(1), 335–357.
- 16)** Kinza Yasar. (2016). Information Security (Infosec). <https://searchsecurity.techtarget.com/definition/information-security-infosec> . (17/08/2023).
- 17)** Laflamme, S. (2016). La notion d'identité dans les sciences sociales en Ontario français. *Cahiers Charlevoix*, 11, 73–112. DOI: <https://doi.org/10.7202/1039283ar> .
- 18)** Latsiou, A., Lambrinoudakis, C. (2026). Cyber Supply Chain Risk Management: From Threats to Treatment. *International Journal of Information Security*, 25, 40. DOI: <https://doi.org/10.1007/s10207-025-01207-9> .
- 19)** Lynch, K. (1984). A theory of good city form. Cambridge, Massachusetts, and London, England: The MIT Press. <https://mitpress.mit.edu/9780262120852/a-theory-of-good-city-form/> .
- 20)** Maurya, U. K., Mishra, P. (2012). What is a brand? A perspective on brand meaning. *European Journal of Business and Management*, 4(3), 122–133. <https://www.iiste.org/Journals/index.php/EJBM> .
- 21)** Melewar, T. C., Bassett, K., Simões, C. (2006). The role of communication and visual identity in modern organisations. *Corporate Communications: An International Journal*, 11(2), 138–147. DOI: <https://doi.org/10.1108/13563280610661679> .
- 22)** Melnyk, S. A., Schoenherr, T., Speier-Pero, C., Peters, C., Chang, J. F., Friday, D. (2022). New challenges in supply chain management: Cybersecurity across the supply chain. *International Journal of Production Research*, 60(1), 162–183. DOI: <https://doi.org/10.1080/00207543.2021.1984606> .
- 23)** Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., Giannakopoulos, G. (2014). The human factor of information security: Unintentional damage perspective. *Procedia – Social and Behavioral Sciences*, 147, 424–428. DOI: <https://doi.org/10.1016/j.sbspro.2014.07.133> .
- 24)** Whitman, M. E., Mattord, H. J. (2018). *Principles of Information Security*, Sixth Edition. USA: Kennesaw State University.
- 25)** M'zungu, S. D., Merrilees, B., Miller, D. (2010). Brand management to protect brand equity: A conceptual model. *Journal of Brand Management*, 17(8), 605–617. DOI: <https://doi.org/10.1057/bm.2010.15> .
- 26)** OECD. (2008). *The Economic Impact of Counterfeiting and Piracy*. Paris: OECD Publishing. https://www.oecd.org/en/publications/the-economic-impact-of-counterfeiting-and-piracy_9789264045521-en.html .
- 27)** OECD/EUIPO. (2025). *Mapping Global Trade in Fakes 2025: Global Trends and Enforcement Challenges, Illicit Trade*. Paris: OECD Publishing. DOI: <https://doi.org/10.1787/94d3b29f-en>.

- 28)** Ou, S., Yang, Q., Liu, J. (2024). The global production pattern of the semiconductor industry: an empirical research based on trade network. *Humanities and Social Sciences Communications*, 11. DOI: <https://doi.org/10.1057/s41599-024-03253-5> .
- 29)** Pecht, M., Tiku, S. (2006). Bogus: Electronic manufacturing and consumers confront a rising tide of counterfeit electronics. *IEEE Spectrum*, 43(5), 37–46. DOI: <https://doi.org/10.1109/MSPEC.2006.1628506> .
- 30)** Phillips, B. J., McQuarrie, E. F., Griffin, W. G. (2014). The face of the brand: How art directors understand visual brand identity. *Journal of Advertising*, 43(4), 318–332. DOI: <https://doi.org/10.1080/00913367.2013.867824> .
- 31)** Rebelo, S. M., Martins, T., Rebelo, A., Bicker, J., Machado, P. (2022). Using computational approaches in visual identity design: A visual identity for the design and multimedia courses of Faculty of Sciences and Technology of University of Coimbra. *arXiv*. DOI: <https://doi.org/10.48550/arXiv.2209.03420> .
- 32)** Rúsbel Domínguez Domínguez. (2023). Evaluation of an information security management system at a Mexican higher education institution. Cornell University. <https://arxiv.org/abs/2306.11050> .
- 33)** Singh, A., Vaish, A., Keserwani, P. K. (2014). Information security: Components and techniques. *International Journal of Advanced Research in Computer Science and Software Engineering*, 4(1), 1072–1077.
- 34)** Taylor, A. (Ed.), Alexander, D., Finch, A., & Sutton, D. (2008). *Information Security Management Principles: An ISEB Certificate*. British Computer Society (BCS).
- 35)** van den Bosch, A. L. M., de Jong, M. D. T., Elving, W. J. L. (2006). Managing corporate visual identity: Exploring the differences between manufacturing and service, and profit-making and nonprofit organizations. *Journal of Business Communication*, 43(2), 138–157. DOI: <https://doi.org/10.1177/0021943605285476> .
- 36)** Van den Bosch, A. L. M., Elving, W. J. L., de Jong, M. D. T. (2006). The impact of organisational characteristics on corporate visual identity. *European Journal of Marketing*, 40(7/8), 870–885. DOI: <https://doi.org/10.1108/03090560610670034> .
- 37)** Wilson, J. M. (2022). Building and Optimizing a Brand Protection Program: A Total Business Solution Model. In J. M. Wilson (Ed.), *Brand Protection and the Global Risk of Product Counterfeits: A Total Business Solution Approach* (pp. 19–36). Cheltenham, UK: Edward Elgar Publishing.
- 38)** Wilson, J. M., Grammich, C., Chan, F. (2016). Organizing for brand protection and responding to product counterfeit risk: An analysis of global firms. *Journal of Brand Management*, 23(3), 345–361. DOI: <https://doi.org/10.1057/bm.2016.12> .