

Impersonating the Visual Identity of the Brand and Ways to Combat It by Strengthening the Information Security System (Analytical Study of Economic Institutions)

Received date: 21/06/2024 Accepted date:28/10/2024 Published date:31/10/2024

Tahar abdessamia ¹, Chaaban hanan ²

¹ *The Laboratory of Uses and Reception of Media and Cultural Products in Algeria, University of Algiers 3, Algeria,*

Email :tahar.abdessamia@univ-alger3.dz

² *University of Algiers 3, Algeria,*

Email :chaaban.hanan@univ-alger3.dz

Abstract:

It is clear that any economic enterprise has a visual identity that distinguishes it from other institutions. An organization cannot succeed if it fails to establish its visual identity in the minds of its audience and build its relationship with each individual through its visual discourse, and this is even more important in light of the technological development through which it is possible to communicate by modern means. However, it is noted that some organizations lack the same care in protecting their visual identity as they dedicate to information security systems to protect their physical, financial and information property, which poses a challenge.

For this reason, our study aims to shed light on the means of protecting organizations' visual identity. This includes monitoring both physical and electronic activities. Although organizations care about displaying their visual identity, they often lack clear strategies to protect it. Common solutions rely on open doors, warning notices, and, in some cases, legal action in the event of trademark infringement by the organization.

Keywords: Visual identity; information security system; Economic institutions.

Corresponding Author: Tahar Abdessamia, **Email:**

tahar.abdessamia@univ-alger3.dz

1. INTRODUCTION:

Major economic institutions emphasize marketing their visual identity to internal and external audiences, leveraging the latest information and communication technology. Their strength lies in being pragmatic and transparent, benefiting other companies and economic institutions. In a market where reputation, image, and core beliefs are more crucial than the product itself, achieving this requires an effective communication approach.

This approach helps economic institutions measure and enhance their relationship with their environment, aiming to be influenced rather than being the influencer. Globally, these institutions focus on maintaining their market position by strengthening their visual identity and defining a specific stereotype. This elevates their relationship from mere transactions to one of communication, trust, and belonging.

The visual identity of an institution guides individuals from cognitive awareness to persuasion, action, and preference, reflecting its values and characteristics through elements like logos, names, and colors (Othmani, 2018, p. 144). This identity is also visible in office supplies, advertisements, websites, transportation, company vehicles, buildings, and display windows. Packaging significantly showcases the visual identity (Annette Bosch, Jong, & Elving, 2006, p. 139).

On the other hand, Visual identity theft poses one of the greatest risks to economic institutions, causing millions of dollars in losses due to the theft of designs, trademarks, shapes, and colors by other entities. These entities, which may be direct competitors or fraudulent organizations operating covertly, exploit the reputation of well-established institutions by mimicking their profiles, backgrounds, appearances, or content. To prevent visual identity theft, many institutions maintain their information security by **Oct Oct**



implementing strategies and systems that control their data and communication networks, preventing external breaches and unauthorized manipulation.

Our study aims to shed light on combating visual identity theft by activating the information security system in economic institutions, the risks they face that threaten their information security, and the reasons that lead to continuous vigilance to prevent this phenomenon. It also discusses the implementation of a set of measures to reduce risks and threats and the national and international protection mechanisms.

From this perspective, we pose the following problem:

❖ To what extent does the information security system within economic institutions contribute to protecting their brand's visual identity from impersonation?

2. SUB-QUESTIONS:

Arising from this main issue are the following sub-questions:

❖ What is the impact of visual identity on improving the mental image of economic institutions?

❖ What is the role of the information security system within economic institutions?

❖ What challenges do institutions face concerning the impersonation of their brand's visual identity?

❖ How have major global institutions dealt with combating various forms of visual identity impersonation?

3. IMPORTANCE OF THE STUDY:

The importance of the study lies in highlighting information security, which has become highly significant for economic



institutions in an era where information is considered intellectual capital and the foundation of digital transformation in the economic and social environment. Information is a strategic source for any decision made by senior management. The study emphasizes the vital roles that economic institutions play through their visual identity and their position in society and the market. These institutions possess specialized material and human resources that qualify them to be leaders in the field of information security and the implementation of protection systems, which the study will detail.

4. OBJECTIVES OF THE STUDY:

The objectives of this study are as follows:

- To identify the impact of visual identity on improving the mental image of economic institutions.
- To understand the role of information security systems within economic institutions.
- To identify the challenges faced by institutions regarding the impersonation of their brand's visual identity.
- To understand how major global institutions combat various forms of visual identity impersonation.

5. METHODOLOGY AND DATA COLLECTION TOOLS:

In this study, we adopted the descriptive-analytical method, which aims to describe the phenomenon of visual identity theft in economic institutions and explore ways to counteract it through information security. The method also focuses on the potential risks in the event of a breach and how to handle the related data. We used observation as a tool for collecting and analyzing information.

6. STUDY LIMITS:

The study's scope is centered on analyzing the brand of some global institutions and the characteristics that distinguish them. Consequently, the results of the study can be generalized and applied to national institutions, benefiting from its outcomes. In line with these considerations, the study was conducted by researching the archives and physical evidence of those institutions.

7. STUDY STRUCTURE:

This study is divided into four sections, as follows:

FIRST: FUNDAMENTALS OF VISUAL IDENTITY IN ECONOMIC INSTITUTIONS

Visual identity is among the dimensions of significant interest to researchers and specialists. Due to continuous advancements in information technology and communication, new communication patterns have emerged, relying heavily on visual images and video with high-definition production and flexible output techniques. This has led to the development of new methods in highlighting the visual identity of economic institutions. Therefore, it is essential to delve into the concept of visual identity, its key functions, and its importance in defining economic institutions.

1.1. Definition of Economic Institution:

Since we are discussing the visual identity of economic institutions, it is essential to define what an economic institution is and its key characteristics:

An economic institution is an independent economic and social organization where decisions are made regarding the composition of human, financial, material, and informational resources to create added value according to specific objectives in a temporal and spatial context. It is an economic unit engaged in productive activities and

related functions such as storage, purchasing, and selling to achieve the institution's intended goals (Ramashe, 2008/2009, p. 25).

Economic institutions are also recognized as democratic entities that engage their internal audience in economic activities by providing factors of production to the market or investing in commercial activities to generate profits (Samarasinghe, 2019, p. 03).

1.1.1. Characteristics of Economic Institutions:

Economic institutions exhibit a set of characteristics that can be summarized as follows (Zaqai, 2009/2010, p. 04):

- Legal personality: Economic institutions have independent legal rights, powers, duties, and responsibilities.
- Capacity for production: They are capable of producing goods or performing functions for which they were established.
- Sustainability: Economic institutions can sustain themselves with adequate financing, favorable political conditions, and sufficient labor, and they can adapt to changing circumstances.
- Clear definition of goals, policies, programs, and work methods: Every institution sets specific goals to achieve, both quantitative and qualitative, related to production and achieving specific business figures.
- Ensuring financial resources to sustain its operations, either through credits, revenues, loans, or a combination of these elements depending on the circumstances.
- Environmental responsiveness: The institution must adapt to its surrounding environment, where favorable or adverse conditions can impact its performance.
- The institution is a fundamental economic unit in the economic

society. In addition to contributing to production and national income growth, it serves as a source of livelihood for many individuals.

- The term "institution" necessarily includes the idea of its potential demise if its justification for existence weakens or its efficiency declines.

1.2. Definition of Visual Identity:

Visual identity is defined as a set of objectives that an organization aims to establish and maintain in the minds of customers through trademarks, logos, color schemes, typography, and slogans, as well as voice elements. These components collectively provide a system for identifying an entity (Rebelo et al., 2019).

A new type of visual identity, known as dynamic visual identities, has emerged due to modern information and communication technology. These identities engage with the public interactively, aiming to create psychological and social connections beyond material interests, making the design of visual identity more complex (Rebelo et al., 2019).

Visual identity includes structural elements like logos, trademarks, colors, and typography styles. Over time, the scope of visual identities has evolved, strengthening and establishing visual identity systems, particularly since the 1950s (Rebelo et al., 2019).

Practically, visual identity is a communication tool for institutions like Condor Algerian, embodying values, behaviors, and visions through symbols, shapes, colors, typography, images, or videos, whether static or dynamic.

1.3. Elements of Visual Identity:

The visual identity consists of several elements that can be summarized as follows:



1.3.1. The Name: The name of the institution holds paramount importance above all other elements that constitute the visual identity. There are two reasons for this importance:

- **Firstly:** The name describes the institution, what it does, and what its aspirations symbolize, etc. Without a name, the institution loses all its structural characteristics, as these elements are interconnected rather than separate. The first of these elements is the name, without which we cannot term it an institution.
- **Secondly:** The name is generally the first point of contact between the institution and its audience (Ilham & Saadi, 2017, p. 193). Without it, there would be no communication, as the sender in this case would be unknown.

Thus, the name is the first thing that meets and circulates among the general public, becoming ingrained in the depths of memory. Brand names can help consumers remember important information about the product (Mariam & Qarnani, 2021, p. 141).

1.3.2. The Logo (Brand): There is a great deal of confusion among many dealing with the subject of visual identity, as they believe it refers to the brand. This is a mistake because the brand refers to the value obtained by the user when dealing with you, while the visual identity is the user's guide to understanding this value.

The brand can be just bright lights or metaphorical shapes like a geometric, archaeological, or animal figure. There is no communication policy without a symbolic form that embodies the institution's identity and acts as a mediator between it and its internal and external environment (Mariam & Qarnani, 2021, p. 141).

The levels of the logo can be defined according to Dr. Nermin Alaa El Din into three levels as follows:

A- **Iconic or Symbolic:** These symbols or marks may be animals, insects, fruits, mythical creatures, or objects that can be embodied in daily life, or symbols inspired by various activities.

B. **Logotype:** It is a representation using letters, numbers, or words to create a unique identity.

C. **Complex Logo:** This involves using words and symbols in an integrated concept.

Symbolizing a logo is a highly complex topic because it relies on the interplay of many elements such as signs, colors, words, and shapes to create a unique and expressive identity at the same time (Nermin, 2022, p. 52).

1.3.3. Typography: This refers to the written treatment of space, with or without printing, and is related to its chronological, historical, and cultural sequence. It is of great importance within the scientific strategy of image and identity (Mariam & Qarnani, 2021, p. 141).

The use of typography in logo design is of great significance, as many logo designs rely primarily on typography. This style of logos is the most widespread, characterized by diversity according to the variety of font design styles. Typographic logos often feature clarity and rapid reach to the recipient (Al-Atoom, 2018, p. 10).

1.3.4. Slogan (sometimes referred to as the baseline): It is a verbal phrase that expresses a goal or idea, characterized by simplicity and clarity. The repetition of the slogan in the consumer's mind aims to increase the likelihood of recall and build a degree of consumer loyalty (Mariam & Qarnani, 2021, p. 141).

Regarding this element, it is a linguistic form associated with the identity name (often very short and characterized by rhythm or even phonetic sound for easy memorization). It tends to be associated with

a linguistic dimension more than a visual dimension of the brand. However, it generally offers a graphic contrast that is usually integrated into the visual expression of the identity, often in very close proximity to the logo or name (Kerret, 2019, p. 21).

1.3.5. Colors: Colors play a pivotal role in bringing the visual aspect to life, acting as the soul that animates the visual identity. For instance, Condor Algeria uses light blue and white colors, where blue represents professionalism, perfection, and trust, and white symbolizes nature, transparency, and integrity.

Colors are chosen based on their psychological and cultural impacts, influencing the audience's impression of the institution.

On the internet, a diverse and vibrant color palette is often used to make sites attractive. However, using too many colors can cause overload and visual discomfort. It is recommended to maintain aesthetic harmony by preserving overall color balance (Kaminski, 2017, p. 20).

1.3.6. Voice: The term "voice" refers to the tones used in communication with the audience, including musical sounds in video clips, advertisements, and audio communications like phone responses or radio ads. These sounds reinforce corporate identity and deepen brand impact.

While "voice" typically relies on hearing and visual identity on sight, the term "voice" in this context refers to creating an identity through language communication. The speech should be attractive and contain sounds that readers can feel, relying on the skills of individuals or communities.

Specialists evoke these sounds based on two requirements:

- Origin of the Speech: This involves the linguistic origin of the words

used, such as various living languages or local and regional dialects.

- Pronunciation: Understanding how words are pronounced in specific regions or dialects helps capture the melody of the speech. For example, in Algeria, "Laghout" is pronounced "Laqwat," and the last letter of each word is often extended.

Integrating the "voice" element complements visual identity, enriching the overall brand experience and making it more memorable and impactful.

SECONDLY: THE NATURE OF INFORMATION SECURITY

2.1. Concept of Information Security (IS):

Information security is defined by specialists as a science that explores theories and strategies for protecting information from risks and attacks. It involves tools and procedures to protect information from internal and external threats, ensuring confidentiality and integrity while combating criminal exploitation of systems (Dakhil & Talha, 2016, p. 19).

The Committee on National Security Systems (CNSS) defines information security as the protection of information and its critical elements, including the systems and devices that use and store this information (Whitman & Herbert, 2021, p. 01).

Information security is also recognized as being free from any risk, whether intentional or unintentional harm from adversaries. This necessitates multiple layers of security, including physical, personnel, operational, communications, network, and information systems security, which include the following elements" (Singh, Abhishek, & Kumar Keserwani, 2014, p. 1073):



- a. **Physical Security:** Protecting physical items or objects of the organization from unauthorized access and misuse.
- b. **Personnel Security:** Protecting individuals or groups authorized to access the organization's data and operations.
- c. **Operational Security:** Protecting operational details or a series of specific activities.
- d. **Communications Security:** Protecting communication media, technologies, and content specific to the organization.
- e. **Network Security:** Protecting the organization's networks (Gateway Guardian).
- f. **Information Systems Security:** Protecting information and its critical elements, including systems and devices, is essential for organizations. An Information Management System (IMS) is a strategic plan aimed at safeguarding an organization's data and controlling access to it, ensuring that only qualified individuals can manage this information.

From a technical perspective, Rúsbel Domínguez defines an Information Security Management System (ISMS) as managing risks based on international standards (ISO/IEC 27000). These standards help measure threats and detect vulnerabilities in information systems, aiding managers in making informed decisions. Failure to manage information security effectively can lead to data breaches with negative consequences (Domínguez, Flores Laguna, & A. del Valle López, 2023).

Digital and non-digital information refers to the following:

- **Paper Information Security System (Non-digital):** This term is used to describe a system that retains information on paper rather than on a computer (Cambridge, 2023).

- **Cybersecurity System (Digital):** Cybersecurity is the practice of protecting vital systems and sensitive information from digital attacks. Cybersecurity measures are also known as Information Technology (IT) security, designed to counter threats against systems and network applications, whether these threats originate from within or outside the organization (IntroCybersecurity, 2023).

Most researchers, organizations, and international bodies in information security consider the CIA triad (Confidentiality, Integrity, Availability) to be crucial principles in an information security system (Taylor, David, Amanda, & David, 2008, p. 03):

A- Confidentiality: This principle ensures that information is not disclosed to unauthorized individuals, entities, or processes. Information is often restricted to a limited number of individuals due to its nature, content, or potential legal, financial, or reputational implications. Restricting access to information to those who have a "need to know" is a good practice based on the principle of confidentiality. Controls to ensure confidentiality are a key part of broader information assurance management.

B- Integrity Principle: This refers to maintaining the accuracy and completeness of information. Information is only useful if it is complete and accurate. Often, ensuring these aspects (integrity) of information is critically important, ensuring that only authorized individuals have the appropriate authority to change, update, or delete information. This principle is another fundamental aspect of ensuring information security.

C- Availability Principle: This pertains to the accessibility and use of information upon request by authorized individuals or entities. If information is not available when needed, it cannot be considered information at all. The issue of information availability is an area



witnessing significant technological advancements, which have posed considerable challenges for information assurance specialists in the past.

In an ideal world, all critical information could be securely stored and never accessed except under perfect assurance conditions. However, this is impractical, necessitating a balance between security and information availability.

Additionally, some researchers have added other elements to these three principles, including:

D- Information Reliability: This involves verifying the identity of users and entities when transmitting information.

E- Non-Repudiation: This ensures that parties involved in transactions cannot deny their involvement. This condition is typically verified through what is known as electronic certificates.

F- Access Control: This refers to the ability to access systems and applications via communication links.

Access control ensures that only authorized users can access systems and applications through communication links, maintaining security and preventing unauthorized access.

In the same context, from a legislative perspective, the concept of cybercrime or electronic crime has emerged, addressing the content of information security and methods to combat it through international treaties, legislative laws, and decrees.

Cybercrime includes any crime committed using a computer system or network. International treaties, legislative laws, and decrees have been established to combat these crimes, enhancing information security.

For instance, the United Nations at its Tenth Congress on Crime Prevention and Criminal Justice held in Vienna in 2000 defined cybercrime as "any crime that can be committed using a computer system or computer network, including initially all crimes that can be committed in an electronic environment" (Al-Wahab, 2016/2017, p. 24).

The United Nations defines cybercrime as crimes committed using computer systems or networks, encompassing all electronic environment crimes. This definition was established at the Tenth Congress on Crime Prevention and Criminal Justice in Vienna in 2000.

In this regard, the Algerian legislator has implemented various texts to combat electronic crime, embodied through Law 09-04 dated May 9, 2009, which includes specific rules for preventing and combating crimes related to information and communication technologies (Hamoudi, 2020, p. 96).

Algeria has enacted laws to combat electronic crimes, such as Law 09-04 dated May 9, 2009, which sets specific rules for preventing and combating crimes related to information and communication technologies.

Ultimately, it can be acknowledged that an information security system is based on fundamental concepts summarized in the following points (Whitman & Herbert, 2021, p. 13):

- **Access:** The ability of a user to access information, where they possess legal permission to access the system. Without this legal permission, access to such information is not possible.
- **Asset:** The organizational resource that is protected can be either logical, such as a website owned by the enterprise, software information, or data, or it can be physical, such as a person, computer

system, or device. Especially, information assets are the focus of security efforts aimed at protecting them.

- **Attack:** An intentional or unintentional act that may harm or endanger information and the systems supporting it. Attacks can be active or passive, intentional or unintentional, direct or indirect.

- **Monitoring, Protection, or Countermeasures:** Security mechanisms, policies, or procedures that successfully confront attacks, reduce risks, address weaknesses, and overall enhance security within the enterprise.

- **Exploitation:** A technique used to breach a system. This term can refer to an action or a name where threat actors attempt to unlawfully exploit another system or information asset for personal gain. Exploitation operations utilize existing software tools or on-demand software components based on the security vulnerability or exposure, which are either inherent in the software or created by the attacker.

- **Exposure Condition:** In information security, exposure occurs when a security vulnerability is known to the attacker.

- **Loss Condition:** In the event of damage or destruction to an information asset.

- **Risks:** The likelihood of an undesirable event occurring, such as a negative event or loss.

- **Subjects and Objectives of the Attack:** A computer can be either the subject of an attack, for example, it can be hacked through an attack by an entity, and then used to attack other systems.

- **Threat:** Any event or circumstance likely to have a negative impact on the organization's information system.

Based on the previous definitions, we can infer that an

information security system aims to protect information and its systems from attacks, whether human-caused or due to natural and material factors. The goal is to ensure confidentiality, integrity, and availability of information when needed. Unauthorized individuals who interfere with this information may face accusations of committing an offense and could be subject to legal consequences and penalties.

2.2 Sources of Information Security Threats:

According to researchers Howard and Benson, there are two main sources (Izki, 2019, p. 39):

A. Natural Disasters Threatening Information Security: Such as floods, fires, and earthquakes.

B. Human Threats: Such as hacking, espionage, and piracy.

Other researchers have also added a source of threat related to material issues like power outages, network failures, or software malfunctions. However, most researchers agree that threats stemming from human behavior pose a significant impact on the success or failure of organizational efforts to secure and protect their operations, services, systems, and information (Metalidou, Catherine, Panagiotis, Niclas, Christos, & Georgios, 2014, p. 426).

2.3. Technical Methods for Information Security System:

There are various means of protection against different threats that an information security system employs, utilizing a set of tools and procedures, including:

1. **Encryption:** This involves a mathematical algorithm where the plaintext is transformed into ciphertext, which cannot be understood until decrypted (Moss, 2022, p. 104).



2. **Segmentation Applications:** These are a collection of applications aimed at ensuring information integrity. They also involve algorithms that secure information exchange.
3. **Electronic Signatures:** This method employs specific techniques to verify transaction owners. Key forms include electronic fingerprints, eye scans, and electronic signatures (Moss, 2022, p. 104).
4. **Password:** No one unauthorized can access the information network without a password. It is one of the simplest forms of protection.
5. **Firewall:** This software protects networks and servers from intruders and infiltrators, constituting a security solution for information technology. It includes setting policies for controlling their permission to access.
6. **Network Address Translation (NAT):** This technology assigns a unique identifier to each device connected to the network, distinguishing them from other devices. Only those authorized by the organization can use these identifiers.
7. **Automatic Update:** This is among the most critical information protection points, given the complexity of system construction. All software programs require updates to enhance security.
8. **Backup Storage:** This copies content and information, preserving it in a secure location for future reference.
9. **Data Erasure:** Most users believe that deleting a file permanently removes it, even from the trash bin. However, this is not accurate because deleting a file from storage deletes the indicator pointing to it, not the file itself. Therefore, it must be erased, with three types: file erasure upon deletion, clearing empty space in storage units, and using the swap file (Dakhil & Talha, 2016, p. 24).

THIRD: CHALLENGES FACING GLOBAL ENTERPRISES REGARDING VISUAL IDENTITY THEFT

3.1. Increasing Cases of Imitation and Counterfeiting (Examples of Some Cases):

Yoland Moutama emphasizes that trademarks are crucial in protecting brand identity, yet unfortunately, this also makes them attractive targets for identity theft. Brand identity theft occurs when an organization uses a trademark (such as a brand name or logo) without permission from the original trademark owner. Some cases of infringement are clear-cut, such as a company directly stealing another company's name or logo. However, sometimes situations take a different turn (Moutama, 2024).

For instance, when the company Yoga sued another company due to similarity in their names (both containing the word "Yoga"). Or when a candy company filed a lawsuit against a rapper because a phrase in his song referenced their product. However, the outcomes of these cases did not favor the larger company, as the smaller party cleverly navigated the legal battle.

In other instances, major corporations direct their legal arsenals against smaller violators to set an example for others.

3.1.1. Apple Records vs. Apple Computer (Now Apple Inc.): The Battle of the Apples: This longstanding battle between the two companies revolves around the rights to the "name". It began in 1978 when The Beatles were at the peak of their creativity and founded Apple Records. The Granny Smith apple logo became the company's symbol. Then, a budding technology company from Silicon Valley decided to name itself Apple as well. The Beatles were not pleased and filed a lawsuit against the technology company for identity theft of their brand identity. The parties eventually reached an agreement



with Apple Computer paying Apple Records a settlement of \$80,000 (VINYL, 2024).

In 2003, Apple launched the iTunes music store, prompting Apple Records to initiate legal action. This culminated in a settlement in 2007, with Apple Inc. securing rights to the Apple Records trademark while Apple Records received \$500 million (Moutama, 2024).

3.1.2. Louis Vuitton vs. Chewy: Protecting Luxury Brand Identity: Louis Vuitton, renowned for its high-end bags priced up to \$10,000, faced imitation when Chewy introduced products adorned with the LV logo. Despite Louis Vuitton's legal protest to stop the infringement, the court ruled in favor of Chewy, finding no evidence that Chewy's pet products would confuse consumers or diminish Louis Vuitton's brand identity (Moutama, 2024).

3.1.3. Monster Energy vs. Monster Fish Keepers: Crossing Industries in Brand Identity: Monster Energy believed they owned exclusive rights to the "Monster" name. In 2012, they sued Monster Fish Keepers, a company manufacturing aquarium filters, citing potential consumer confusion between energy drinks and fish tank equipment. Despite Monster Energy's cease and desist letter, Monster Fish Keepers refused to change their name, arguing they operate in distinct industries (Moutama, 2024).

The common thread across these cases is the difficulty companies face in winning lawsuits alleging visual identity theft of their trademarks. Courts typically require proof of potential consumer confusion, illustrating the complexity of trademark infringement law. Most cases do not favor the plaintiff, prompting global companies to innovate strategies to safeguard their visual identities from imitation and theft.

The rising instances of imitation, counterfeiting, and visual identity theft—from logos to packaging—pose significant threats to businesses, markets, and consumers alike.

Cases of imitation and counterfeiting bring forth a diverse array of challenges and damages. Concerning enterprises, unlawful imitation can lead to deterioration of their identity and consumer perception. Customers are misled into purchasing products that appear genuine but are actually low-quality imitations. Furthermore, such instances can diminish incentives for innovation, as original enterprises find themselves unfairly competing against imitators.

3.2. Identity Counterfeiting in E-commerce and Digital Markets:

E-commerce and digital markets represent among the most prominent transformations witnessed in the global economy in the 21st century. Despite the significant benefits these technologies bring, they face a set of prominent challenges relating to the nature of business and commerce in the digital age.

One of the foremost challenges is the increasing prevalence of counterfeiting and imitation in the digital market. With greater access to e-commerce platforms, unauthorized entities can swiftly and easily launch counterfeit products and false offers. This not only impacts original enterprises and their reputation but also affects the internal communication of visual identity among employees.

3.2.1. Identity Counterfeiting in Electronic Banking Services (also known as e-banking): Electronic banking services represent a visible transformation in the era of Technology 4.0 for banks worldwide. These services are also referred to by various names such as "virtual banks," "online banks," "cyber banks," "web banks," "phone banks," and "remote electronic banks." Electronic banking

services encompass all forms of transactions between banks and customers based on processing and transmitting digital data to provide banking services online (Le, Do Thu, & Mai Khanh, 2023, p. 61).

The fear of identity counterfeiting online triggers negative emotions among consumers, activated through their cognitive assessment/personal ideas about the potential theft of personal and financial data during online transactions (Hille, Walsh, G, & Cleveland, M, 2015, p. 02). This occurs concerning the relationship between fears of digital identity theft by banks and concerns about security breaches and client privacy.

3.2.2. Challenges of the European Union in E-commerce through Brand Identity Counterfeiting: Customs offices in European Union countries have recorded seizure cases related to online sales of goods, identified by customs officials in each case, taking into account accompanying documents. However, the collection and provision of internet sales data vary from country to country within the European Union, with some countries reporting the majority of seizures associated with online sales, while no seizures are recorded in other countries during the period from 2017-2019. It is noted that most counterfeit products destined for the European Union were purchased online, representing 60% of global seizures from 2017 to 2019. Despite this, online sales accounted for only a small percentage of 11% of the total seized value (Trade, 2022, p. 65).

However, this percentage increased significantly after the COVID-19 crisis, with the rate of seizure of counterfeit products from online sales reaching approximately 30% by 2023 (Trade, Illicit Trade in Fakes under the COVID-19, 2024, p. 17).

In general, e-commerce and digital markets require comprehensive strategies to deal with these challenges. Institutions

must adopt best practices in terms of security, quality, and marketing to achieve sustainable development and meet consumer expectations in this rapidly changing digital age.

FOURTHLY: MECHANISMS TO COMBAT VISUAL IDENTITY THEFT THROUGH INFORMATION SECURITY SYSTEMS

Approaches to combating identity theft vary from one institution to another, depending on the institution's size, the mechanisms employed, and the extent of the threats faced by the institution. For instance, Condor, the Algerian institution, employs a range of measures to protect its visual identity.

4.1. Intellectual Property Protection:

In a competitive business world, whether the competition is fair or unfair, visual identity serves as a benchmark to distinguish between what is good and bad in marketplaces. To protect itself from any illegal activities that other parties or entities may undertake by exploiting its trade name and trademark, the institution develops a completely unique visual identity and legally registers it with the relevant authorities in the country.

Condor's website, along with all copyrights, trademarks, and intellectual property rights, belongs to Condor. No third party is allowed to reproduce, distribute, or modify the content in any commercial manner unless necessary for displaying related content for non-commercial purposes.

Furthermore, the institution has implemented measures to promptly address any suspicion of misuse of its visual identity or infringement of intellectual property rights by another party. Immediate contact with the institution will lead to necessary actions to stop such violations.



The trademarks and logos used on the institution's website are the property of Condor or its licensors, and their use requires prior authorization. In case of breaches, Condor reserves the right to demand cessation of unlawful use or correction, and may take legal action against the infringing entity if the violation persists.

4.2. Application of Advanced Detection Technologies:

Advanced detection technologies serve as a proactive solution to combat visual identity theft within Condor, the Algerian institution. By utilizing the latest available technologies and tools, the institution can enhance its capability to accurately and effectively identify and analyze counterfeit products and false claims.

These technologies include the use of image and video recognition systems, where the institution can apply sophisticated AI-based techniques to detect even slight changes in product designs or trademarks. These technologies involve precise comparison and analysis of images, enabling the detection of subtle differences that may be difficult to discern with the naked eye.

Additionally, the use of sensing and analysis technologies helps in detecting changes in materials and components used in product manufacturing. Techniques such as spectroscopy are applied to identify chemical components of materials and compare them with authorized ones.

Through the use of these advanced detection technologies, Condor can enhance the quality of its products and prevent the spread of counterfeit products in the market, thereby protecting its reputation and enhancing customer trust.

4.3. Establishment of Continuous Monitoring and Surveillance System:

Establishing a continuous monitoring and surveillance system for visual identity theft is a fundamental step in maintaining the institution's reputation and protecting its products. This system involves identifying and monitoring suspicious and unusual activities across various channels and platforms where the institution operates.

By using analytical and data technologies, the institution can track patterns and abnormal behaviors that may indicate identity theft operations. It can also monitor changes in sales patterns, consumption reports, and interactions on social media platforms, aiding in the detection of unauthorized changes.

Furthermore, establishing an effective monitoring system requires identifying the resources and tools that contribute to implementing this system. Data management and analysis systems can be utilized to effectively analyze data, guide efforts, and verify the success of implemented measures.

4.4 Enhancing Data and Communication Security:

To effectively combat visual identity theft, it is crucial to enhance data and communication security within the institution. This includes implementing advanced encryption technologies to protect sensitive data from unauthorized breaches.

Security enhancement strategies should encompass multi-factor authentication procedures to ensure that only authorized individuals can access sensitive information, along with access control measures. Data security aspects also involve protecting digital infrastructure and networks from cyber attacks and intrusions.

Achieving data and communication security enhances the institution's ability to protect its sensitive information and products from visual identity theft, thereby building customer trust and maintaining its reputation.



8. STUDY FINDINGS:

If the aim of the study is to combat visual identity theft through activating an information security system in economic institutions, it has yielded a series of findings that can be discussed as follows:

- The visual identity on the institution's website plays an important role as a means of conveying the semantic message that addresses the recipient's emotions. The designer of this identity considered showing the institution by allocating the largest space on the website to display advertising flashes for products.
- The issue of visual identity theft does not receive significant attention from economic institutions when using an information security system; rather, the form of protection is implicit and not originally intended for protection.
- Protecting the visual identity falls under the protection of intellectual property, whether through designing the trademark and logo or through using electronic attributes.
- Among the methods used to protect the institution's visual identity are security-enhancing strategies, including multi-factor authentication procedures to ensure that only authorized individuals can access sensitive information and access control measures. Data security aspects also lie in protecting the digital infrastructure and networks from cyberattacks and breaches.

9. CONCLUSION:

Continuous digital transformation and rapid technological advancements underscore the critical importance of activating information security systems to combat visual identity theft within economic enterprises. Implementing advanced, technology-based strategies helps organizations safeguard their reputation and integrity,

ensuring their products and services remain secure from counterfeiting and imitation.

The study highlights that activating an information security system involves a comprehensive set of integrated measures. These include advanced detection technologies to discern precise differences between original and counterfeit products, continuous monitoring systems to track unusual and suspicious activities, and robust encryption and protection technologies for sensitive and critical data.

Implementing these measures helps build a trustworthy and secure visual communication environment, enhancing an organization's ability to maintain meaningful relationships with consumers, clients, and employees. These initiatives bolster market confidence and enhance the reputation of companies and institutions.

Combating visual identity theft through information security systems also delivers economic and social benefits, such as enhancing competitiveness, fostering innovation, and improving the quality of services and products. Activating an information security system is a crucial step toward achieving a sustainable and reliable business environment in the age of technology and digitalization.

The study provides recommendations for institutions to enhance the protection of their visual identity from impersonation:

Invest in modern technologies related to software and specialized technical expertise, establishing a dedicated database to monitor activities effectively.

Conduct regular training courses for employees to raise awareness about the risks of visual identity theft, how to deal with stolen identities, and how to recognize perpetrators, alongside training on how to respond when identity theft is detected.



Employ electronic protection technologies utilizing monitoring and surveillance systems for counterfeit activities on the internet and within internal systems of the organization.

Regularly compile and review security reports and records, relying on accurate statistics and continuous assessment to pinpoint and address specific vulnerabilities. Conduct periodic evaluations of security policies and procedures, refining them based on previous experiences and changes in security threats.

BIBLIOGRAPHY LIST:

1. Books:

1) Kerret, G. d. (2019). L'identité visuelle des musées à l'ère des marques. Paris: La Documentation française.

2) Taylor, A., David , A., Amanda , F., & David , S. (2008). Information Security Management Principles. Scotland: The British Computer Society.

3) Trade, I. (2022). Dangerous Fakes: Trade in Counterfeit Goods that Pose Health, Safety and Environmental Risks. paris: OECD Publishing.

4) Trade, I. (2024). Illicit Trade in Fakes under the COVID-19. paris: OECD Publishing.

5) Whitman, M. E., & Herbert , J. (2021). Principles of Information Security (Sixth Edition ed.). Boston: Cengage Learning Customer & Sales Support.

2. Theses:

6) Diab Zaky. (2009/2010). Business Communication and Its Effectiveness in Economic Institutions. Doctoral Thesis in Economics, Faculty of Business and Management Sciences, University of Abi Bakr Belkaid. Tlemcen.

7) Emad Yasser Youssef Al-Atoum. (2018). Degree of Achieving Visual Identity in Designing Logos of the University of Jordan. Master's Thesis in Graphic Design, Faculty of Architecture and Design, Middle East University, Jordan.

8) Izki, F. H. (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. A thesis submitted in fulfilment of the requirements For the degree of Doctor of Philosophy, Department of Computer and Information Sciences, University of Strathclyde .

9) Kaminski, É. (2017, jul 05). Comment développer sur le web une identité visuelle dont le but est de promouvoir son propre univers ? Lille, Mémoire de Master deuxième année Ingénierie Documentaire Edition et Médiation Multimédia, Universitaire Lille III.

10) Mliani Abdelwahab. (2016/2017). Information Security in the Electronic Business Environment. Doctoral Thesis in Law, Faculty of Law and Political Science, University of Abi Bakr Belkaid. Tlemcen.

11) Sabrina Ramash. (2008/2009). Communication Effectiveness in Algerian Economic Institutions. Doctoral Thesis in Sociology, specializing in Development and Human Resource Management, Faculty of Humanities and Social Sciences, Mentouri University. Constantine.

3. Printed article:

12) Annette Bosch, L. M., Jong, M. D., & Elving, W. J. (2006). MANAGING CORPORATE VISUAL IDENTITY. Journal of Business Communication(43).

14) Ahmed Nouri Dakhil, Saad Abdul Salam Talha. (June, 2016). Information Security Breaches and Avoidance Methods. International Journal of Engineering and Information Technology, 02(02).

15) Alaa Eldin Nermin. (December, 2022). Representing Dimensions of National Identity in Visual Designs of Major Sports Events: A Study Applied to the World Cup. Scientific Journal of Public Relations and Advertising Research, 03(24).

16) Bushmuha Ilham, Wahida Saadi. (June, 2017). Institutional Visual Identity and Branding Between Creativity and Achieving Competitive Advantage. History of Science Journal, 02(02).

18) Fareeda Hamoudi. (July, 2020). Information Security in Algeria Between Technological Developments and Digital Environment Weakness:



A Legal Study on the Banking Sector. Deep Legal Research Generation Journal, 41.

19) Hille, P., Walsh, G, & Cleveland, M. (2015). Consumer fear of online identity theft: Scale development and validation. Journal of Interactive Marketing, 30(01).

20) Karima Othmani. (2018). Institutional Visual Identity: The Challenge for Economic Institutions in Brand Definition - A Field Study at Condor Electronics. Algerian Journal of Studies and Research, 01(02).

21) Kamal Masous. (2022). Information Systems Governance Practices in Enterprises: Acceptance or Mitigation of Electronic Attacks. Algerian Journal of Globalization and Economic Policies, 13.

23) Le, T. T., Do Thu , H., & Mai Khanh , N. (2023). the impact of online identity theft on customers' usage intention of e-banking transactions in uncertain context. Journal of Governance and Regulation, 12(04).

24) Mariam B., Qurnani Y. (2021). Representations of the Visual Identity of the Mobilis Brand in Television Advertising. Journal of Aesthetics, 08(02).

25) Metalidou, E., Catherine , M., Panagiotis , T., Niclas , E., Christos , S., & Georgios , G. (2014). The Human Factor of Information Security: Unintentional Damage Perspective. Procedia Social and Behavioral Sciences, 147.

26) Othmani Karima. (2018). Visual Identity: The Challenge for Economic Institutions in Brand Definition. Algerian Journal of Research and Studies, 01(02).

27) Phillips, B. J., Edward , F., & W. Glenn , G. (2014). The Face of the Brand: How Art Directors Understand Visual Brand Identity. Journal of Advertising, 43(04).

28) Singh, A., Abhishek , V., & Kumar Keserwani, P. (2014). Information Security: Components and Techniques. International Journal of Advanced Research in Computer Science and Software Engineering, 04(01).

3. Seminar article:

29) Rebelo, S. M., Martins, T., Artur , R., João , B., & Penousal , M. (2019, Octobre 22–23). 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. Paper presented in 10th Typography Meeting “Borders”. Matosinhos, Portugal.

4. Internet websites:

30) Cambridge. (2023). Meaning of paper-based,. Consulté le 08 17, 2023, from <https://dictionary.cambridge.org/dictionary/english/paper-based>.

31) Domínguez, R. D., Flores Laguna, O., & A. del Valle López, J. (2023, 08 20). Evaluation of an information security management system at a Mexican higher education institution. Retrieved 06 06, 2024, from <https://arxiv.org/abs/2306.11050>.

32) IntroCybersecurity. (2023). IntroCybersecurity. Retrieved 08 17, 2023, from https://www.romanianunitedfund.org/intro_cybersecurity?gclid=CjwKCAjwivemBhBhEiwAJxNWN1E5ChapjAfFx0oAIBJFVZee02AHgKJ_FAqnkFxNoBN_y6bZxW8n5BoCoOMQAvD_BwE.

33) Moutama, Y. (2024, 03 07). Trademark Madness: 5 Wild Cases of Brand Identity Theft. Retrieved 06 07, 2024, from <https://www.digip.com/blog/post/trademark-madness-5-wild-cases-of-brand-identity-theft>.

34) Samarasinghe, T. (2019, December 22). The relationship between institutions and economic development. Retrieved 06 08, 2024, from <https://mpira.ub.uni-muenchen.de/97755/>.

35) VINYL, B. (2024, 02 06). The Battle of the Apples: The Epic Legal Saga of Apple Corps v. Apple Computer. Retrieved 06 07, 2024, from <https://atlasrecords.co.uk/blogs/all-about-vinyl/the-battle-of-the-apples-the-epic-legal-saga-of-apple-corps-v-apple-computer>.