DIGITAL FRAUD

campos thomaz
& meirelles advogados

INDEX:

1 INTRODUC-

— What is Digital Fraud?

raud is a cunning, deceptive, and bad-faith act that aims to harm or deceive someone to bring some financial advantage to the fraudster over the victim. It can cause irreparable harm to the victim, whether financial, psychological, or image. Fraud covers a complex universe of crimes and penalties in the Brazilian Penal Code.

Digital fraud, more specifically, can be characterized as any situation in which data is misused to commit cybercrimes, causing harm to victims (either consumers or companies).

In the case of companies, digital fraud can also become personal data breaches and cause even more severe consequences.

— Current Scenario

In recent years, the increase in users using digital media has resulted in a rapid adaptation of Brazilian businesses in digitizing their operations. The digital context is favorable to the expansion of crimes due to the greater ease of stealing data and more difficulty in identifying criminals than the physical environment.

The Covid-19 pandemic further accelerated this process. The internet has become increasingly used for different purposes, such as working (home office) and digital transactions due to the social isolation.

Thus, the digital environment has become increasingly seen as an opportunity to apply fraud.

— 2021 Data

Brazil is the 3rd country in the world most affect-ed by fraud

57% of the Brazilian companies are affected by digital fraud*

Most affected sectors: financial institutions, marketplaces, and e-commerces

BRL 5.8 billion in losses from fraud on e-commerce sites, direct sales, financial and telecommunications services**

Only 39% of the companies consider digital security a priority***

* Research published by Instituto Datafolha and MasterCard (https://www.mastercard.com/news/latin-america/pt-br/noti-cias/comunicados-de-imprensa/pr-pt/2021/junho/57-das-empresas-brasileiras-sao-alvos-de-fraudes-e-ataques-digitais-com-alta-ou-media-frequencia-revela-estudo-da-mastercard/#:~:text=Sobre%20o%20Bar%C3%B4metro%20da%20Seguran%C3%A7a,25%20de%20fevereiro%20de%202021.)

** Research published by ClearSale (https://blogbr.clear.sale/mapa-da-fraude-2021-clearsale)De acordo com pesquisa do Instituto Datafolha em parceria com o MasterCard (https://www.mastercard.com/news/latin-america/pt-br/noti-cias/comunicados-de-imprensa/pr-pt/2021/junho/57-das-empresas-brasileiras-sao-alvos-de-fraudes-e-ataques-digitais-com-alta-ou-media-frequencia-revela-estudo-da-mastercard/#:~:text=Sobre%20o%20Bar%C3%B4metro%20da%20Seguran%C3%A7a,25%20de%20fevereiro%20de%202021.)

***Research published by Instituto Datafolha and MasterCard (https://www.mastercard.com/news/latin-america/pt-br/noti-cias/comunicados-de-imprensa/pr-pt/2021/junho/57-das-empresas-brasileiras-sao-alvos-de-fraudes-e-ataques-digitais-com-alta-ou-media-frequencia-revela-estudo-da-mastercard/#:~:text=Sobre%20o%20Bar%C3%B4metro%20da%20Seguran%C3%A7a,25%20de%20fevereiro%20de%202021.)

— Law 14.155/2021 – New penalties for fraud and digital scams in Brazil

Law 14.155/2021 was enacted to respond to the scenario of increased digital fraud committed in Brazil over the last few years. With such a law, cybercrimes such as fraud, theft, and swindling achieved through electronic devices (mobile phones, computers, and tablets) are punished with higher penalties. The main changes promoted by such law include:

- Increased penalty for the invasion of electronic devices (detention went from three months to a year to one to four years)
- Increased penalty for circumstances in which the invasion results in obtaining content from private electronic communications, trade or industrial secrets, confidential information, or the unauthorized remote control of the hacked device (detention went from six months to two years to two to five years and fine)
- The penalties may be increased by one third to two thirds if the crime is committed through a foreign server
- If the crime is committed against the elderly or vulnerable, the penalty may be increased by one-third to double

2 MOST COMMON TYPES OF DIGITAL FRAUD

Phishing

Phishing is considered one of the most common frauds. It is characterized by an attempt to illegally acquire a third party's data, such as passwords, financial data, bank details, or credit card numbers. Phishing usually involves sending a fake link from a bank or a false promotion to users that share data while believing it to be true.

Malware

Malware is a term used to classify all types of malicious software (e.g., worms, spyware, trojan, ransomware) used to cause any damage to the hacked device. Malware can be used to control the computer or for a direct attack, in which malicious code can capture victim's data. Malware can spread in many ways, including through malicious emails (spams), or sending fake files that infect the electronic device when opened.

Ransomware

Ransomware is a malicious code that makes inaccessible data stored on equipment, usually using encryption. In addition to infecting the equipment, ransomware may also encrypt other connected, local, or networked devices. It often requires ransom payment to restore access to the user via bitcoins. Ransomware can spread in many ways, although the most common is through emails with malicious code attached or that induce the user to click on a link.

Shadow IT and equipment theft

"Shadow IT" is the term given to unofficial, unauthorized, and unknown practices by the IT management of a company, such as the use of unauthorized software. Unmonitored use of IT devices can pose security threats to corporate data. Also, theft of corporate or personal equipment containing work data (as in the case of "Bring Your Own Device") can pose severe risks to a company's security.

Invasion by Security Breach

Security breaches open the door to digital fraud. This breach can occur for many reasons, such as a server security breach, the absence of a required system update, or even the lack of server room access control

Fake Bank Slips

This fraud is characterized by sending a fake bank slip to the victim's email on behalf of a known company or institution. The victim, however, believes the banking slip to be genuine (e.g., a ticket for the payment of the electricity or telephone bill).

Identity Fraud by Email and WhatsApp

Sending malicious links by email or WhatsApp has become increasingly common. Criminals send links with matters of public interest to attract victims. By clicking on the fake link and providing the requested data, data is stolen (e.g., registration for emergency assistance during the pandemic of Covid-19). Other scams specifically involve WhatsApp, such as cloning the app account. In this type of fraud, the criminal pretends to be a company representative and requests the WhatsApp verification code sent by SMS to the victim's phone. In possession of the code, the criminal manages to clone the victim's WhatsApp and have access to the list of contacts to ask for money for friends and family of the victim.

Pix (instant payment system) Fraud

Pix (a Brazilian instant payment system) revolutionized banking transactions by enabling transfers or payments in a few seconds without charges. With this new application, new related scams were created. While some are just an adaptation of old deceptions, others exploit the characteristics of the new payment system. One of them, already responsible for the theft of millions of Brazilian reais, is the "failure of the Pix." It promises the user to return twice the money transferred to certain accounts via Pix with the justification of a security failure of a particular financial institution. Many users tend to perform a transfer impulsively. After reflecting on fraud, it is already too late to get the money back.

Fraudes Digitais

To increase Pix's security, the Brazilian Central Bank is creating new tools (such as the Special Return Mechanism (MED) and the Precautionary Blocking) to prevent fraud and assist potential victims. With the Precautionary Blocking, if the bank where the scammer receives the resources distrust an operation, it can assess evidence of fraud and block the resources for up to 72 hours. The Special Return Mechanism can be triggered by both the bank and the victim of the alleged scam. It is necessary to register a police report and report the incident to your financial institution through the official customer service channels. The money goes back to the victim's account if the scam is recognized.

3 INTERNAL SECURITY MEASURES

To prevent digital fraud is necessary to plan, develop strategies, and promote internal training to company employees.

Recognize your vulnerability to attacks: Currently, any organization, regardless of size, is subject to digital fraud. Therefore, recognizing your organization's vulnerability and giving importance to this risk is the first step. After that is possible to identify vulnerabilities and create strategies for the adequacy and training of the company.

Developing a security policy: Developing an information security policy is essential to protect an organization from digital fraud. It shall include, among other aspects, the need to create strong passwords that are frequently changed, general rules for storing documents, making downloads and attachments, and what to do in the event of an incident.

Employee training: In addition to implementing the security policy, it is necessary to promote periodic training to the organization's employees so that they understand the rules clearly and can recognize the scams and know what to do if it occurs.

Data backup: It is essential to backup data periodically, in a secure system, with a reliable cloud service. Thus, if any problems occur, all data is saved elsewhere.

— Practical Tips on How to Prevent Digital Fraud

- Use security mechanisms such as antimalware programs, firewalls, and anti-phishing filters
- Always perform the security updates available on your computer to avoid system vulnerabilities

- Beware emails with suspicious attachments that may contain malicious code or induce the user to follow a suspicious link
- Stay tuned for incoming emails that trick you into providing information, installing/running programs, or clicking links
- Use an effective spam filter. Most emails with malicious files attached are typically identified as spam
- Never write down passwords and other sensitive information in easily accessible places (including unencrypted files inside your computer or flash drives)
- Don't reply to spam emails
- Always check the links sent to you. Scammers often use techniques to mask the actual link to phishing. However, when positioning the mouse on the link, it is often possible to see the exact address of the fake page or malicious code
- Make sure the page uses a secure connection. Trusted e-commerce or Internet Banking sites use secure connections to request relevant data
- Avoid browsing risky websites and never download files from sites you don't know about or are not fully trusted
- Set up your internet to always ask for authorization and confirmation before downloading or running any file or program on the internet

4 HOW TO IMPROVE THE SAFETY OF YOUR CUSTOMER?

It is highly relevant to take measures to prevent security breaches and, consequently, protect a company and its users from fraud and cyber-attacks. Here are some of the actions that you may take:

Keep your antivirus up to date: Always keep an adequate and up to date antivirus in your devices.

Encryption: It is recommended to encrypt data to make data access by third parties more difficult in case of incident.

System update: Always use up-to-date software to prevent the vulnerability of your devices.

Require strong password creation: It is essential to develop strong passwords to administrate servers and websites. Another practice for preserving information is requesting passwords with letters and numbers for users to join certain page areas.

Background Check: There are procedures available (such as background checks) for analyzing information provided by customers, partners, and suppliers to verify if the information provided is accurate and reliable to prevent fraud.

Facial Recognition: Facial recognition technology can help reduce the risks of customer identity fraud. This authentication method uses facial biometric techniques to analyze a user's face, trace patterns, and unique characteristics. It makes it possible to ensure that the person trying to access your platform or perform a financial transaction is them.

5 WHAT TO DO IN CASE OF FRAUD?

— MEASURES TO ADOPT IN THE EVENT OF FRAUD

Even with the adoption of preventive measures to reduce the risk of attacks, at some point, you or your organization may come across digital fraud.

Thus, it is vital to have an incident response plan to guide the management of any fraud or suspected incident quickly and appropriately.

— WHAT TO DO IN CASE OF FRAUD INVOLVING PERSONAL DATA?

When fraud involves unauthorized, accidental, or unlawful access to personal data and may cause a risk to the rights and freedoms of the personal data subject, it may result in a data breach under the Brazilian General Data Protection Act ("LGPD").

— IN THE EVENT OF A DATA BREACH, THE FOLLOWING STEPS SHALL BE OBSERVED:

- Trigger company's incident response plan
- Internally assess the incident, i.e., its nature, category, number of affected data subjects, type and quantity of data involved, concrete, and possible consequences.
- Inform the company’s Data Protection Officer (DPO)
- Notify the data controller (if you are the data processor)
- Notify the Brazilian Data Protection Authority ("ANPD") and the data subject in case of risk or relevant damage to the data subjects
- Prepare documentation including the internal assessment of the incident, measures taken, and risk analysis for complying with the accountability principle

Our recognitions

Análise Advocacia (2021)

Chambers & Partners Brazil (2021 & 2022)

Leaders League (2021 & 2022)

Transactional Track Record (2021 & 2022)

The Legal 500 (2022)

Meet our Partners

Alan Campos Thomaz

Partner

Technology & Digital Business, Privacy and Data Protection, Fintechs and Intellectual Property

at@camposthomaz.com

+55 11 9 8375.2627 +1 (650) 6436652

Sérgio Meirelles

Partner

Corporate, M&A, Venture Capital and Wealth

sergio@camposthomaz.com

+55 11 9 7551.9865

Filipe Starzynski

Partner

Litigation & Law Enforcement, Civil, Real State, Labor and Family

filipe@camposthomaz.com

+55 11 9 7151.9639

Juliana Sene Ikeda

Partner

Intellectual Property, Technology, Agreement and Life Sciences

juliana@camposthomaz.com

+55 11 9 8644.1613

Follow us

Subscribe to our newsletter