GASA
Global Anti-Scam Alliance

Report on the 1st Round Table of GASA Mexico Chapter

INTRODUCTION

On 28 January 2026, the first roundtable discussion of the GASA Mexico chapter was held at Scotiabank's facilities in Mexico City: a foundational milestone in the formation of a coordinated response to the digital fraud crisis affecting the country.

GASA Mexico — the national chapter of the Global Anti-Scam Alliance — was established to catalyze collaboration across sectors to address the digital fraud crisis which, according to GASA's 'State of Scams in Mexico 2025' report, has caused annual economic losses of up to 139 billion pesos, and is only escalating due to the growing sophistication of artificial-intelligence-driven attacks.

The main objective of this first session was to establish a comprehensive national agenda that would unify the efforts of the financial sector, digital platforms, telecommunications companies, the government, and civil society, breaking down institutional silos and creating coordinated response systems.

Meeting attendees included representatives from the financial sector (Scotiabank, Banorte, BBVA, Banamex, and Clip), the digital ecosystem (Microsoft, TikTok, Google, Mercado Libre, and Tools for Humanity), the telecommunications sector (Telefónica and AT&T), the government and regulators (the Ministry of Foreign Affairs, the CNBV, and the Telecommunications Regulatory Commission), the legislative branch (the Senate's Artificial Intelligence Committee and the Chamber of Deputies' Science and Technology Committee), and companies specializing in fraud prevention (Mastercard, Nasdaq Verafin, Feedzai, and VoiSek), as well as civil society organizations such as TechCheck.

During the meeting, the General Directorate of Cybersecurity of the Mexican Government's Agency for Digital Transformation and Telecommunications (ATDT) signed a Memorandum of Understanding with GASA Mexico, officially joining the GASA Mexico Board of Advisors in the national fight against online scams and fraud.

*This document provides a structured summary of the observations, diagnoses, and suggestions offered by participants during the January 28 session. The aim is to articulate a shared vision to guide the coalition's future work, along with examples of what that work **could** entail. It does not represent the views of any individual roundtable participant or final recommendations of the group or of the GASA Mexico Chapter.*

GASA
Global Anti-Scam Alliance

STRATEGIC CONTEXT - WHY MUST WE ACT?

Mexico is at a critical juncture, requiring an immediate transition from a reactive security model to one of '**active co-responsibility**'. Digital fraud is carried out by highly coordinated transnational criminal networks, so defense must be systemic. As one of the two most attractive and vulnerable markets for cybercrime in Latin America, Mexico cannot afford isolated responses. Active co-responsibility is not optional; it is the only approach capable of uniting the financial, technological, and governmental sectors to address attacks that are executed in milliseconds.

The urgency to act is evident in the increasing attack surface. For example, Mexico has grown from 600,000 digital businesses in 2014 to over 6 million today. While this growth is a success in terms of financial inclusion, it has also created a '**digital alternative to cash**' that exceeds institutional oversight capabilities. This massive expansion has eroded systemic trust, allowing digital anonymity to be exploited as a means of evading accountability.

According to the Microsoft Digital Defence Report findings and data from the first half of 2025, the threat magnitude is asymmetrical.

- **A massive volume of attacks:** On Microsoft email services alone, 15.9 billion attack attempts were recorded during this period.
- **Hostile automation:** 1.6 million attempts to create fake accounts are blocked every hour, globally.
- **Regional sophistication and bots:** In the first half of 2025, over 90% of new account requests originated from malicious bots. Mexico and Brazil are home to the most advanced cybercriminals in the region, who use AI to create convincing deepfakes and commit identity theft.

Such a large-scale issue requires a technical diagnosis in order to resolve the current fragmentation before user mistrust causes the digital ecosystem to collapse.

GASA
Global Anti-Scam Alliance

DIAGNOSIS OF INSTITUTIONAL AND OPERATIONAL FRAGMENTATION

The main obstacle to national digital security is the disconnect between technical detection and the subsequent judicial response. Currently, there is a critical bottleneck in the 'legalisation of information' within the investigative file. Although banks and telecoms companies can identify fraud in real time, the protocols for converting technical data such as IP addresses, call logs and bank transactions into valid evidence in court are outdated, which undermines the legal process.

Jurisdictional fragmentation guarantees impunity. In the current model, public prosecutors' offices are limited by physical borders, which is ineffective against digital crime. For example, fraud initiated in Mexico City with deposits in Cancún or through cryptocurrencies mined in international jurisdictions such as India or Brazil leaves local authorities without operational jurisdiction. This institutional disconnect creates a 'fragmentation of trust', whereby users are not only defrauded, but also subjected to bureaucratic 'bullying' by a system that victimizes them further. This results in 48% of complaints to CONDUSEF regarding unauthorized charges never resulting in a criminal complaint.

Cybercrime Network Operation	**Siloed Response from Institutions**
Global collaboration and real-time sharing of tactics among criminals.	Fragmentation of information; banks and telcos do not share source data in an agile manner.
Use of AI to automate mass attacks and evade identity checks.	Manual legal processes; lack of protocols for the "legalization" of digital evidence.
Exploitation of jurisdictional loopholes and territorial borders.	Public prosecutors limited by state powers and territorial bureaucracy.
Extreme agility in mutating attack vectors.	Static regulatory frameworks and lack of technical training for decision-makers.

GASA
Global Anti-Scam Alliance

THE FOUR PILLARS OF THE NATIONAL SHIELD (LEGISLATIVE FRAMEWORK)

Following 72 discussions and over 280 specialist interventions in 2025, the Senate of the Republic defined architecture for a proposed General Law for the Promotion and Regulation of AI. This legal framework aims to transform AI from a threat into a strategic national defence capability by balancing productivity with the mitigation of systemic risks. In the context of this roundtable, the framework offered four relevant pillars to organize ideas suggested by roundtable participants for legislative actions to help counteract the rise of online fraud and scams.

1. Punitive Pillar: The state could update criminal offences to eliminate anonymity as a shield. Legislation could ensure that crimes committed using emerging technologies are punished with the same severity as physical crimes. This would give the federation the necessary 'muscle' to intervene when local capabilities are overwhelmed.

2. Detection Pillar: Mandatory technical collaboration mechanisms could be established to identify deception in real time. This would involve creating a 'shared signals' infrastructure, whereby the detection of a bot or impersonation by a digital platform would trigger immediate alerts within the banking sector.

3. Predictive Pillar: This pillar would form the cornerstone of proactive deterrence. It is based on a regulation published by the National Banking and Securities Commission (CNBV) in June 2024, which has been mandatory since January 2025. It would require financial institutions to implement AI-based transactional behavior analysis systems to block movements that exceed normal limits or exhibit atypical patterns before capital leaves the system.

4. Preventive Pillar (Culture of Prevention): Prevention should evolve from an educational concept for end users and into a training mandate for decision-makers and authorities. For the shield to be successful, legislators, judges and executives will have to build their understanding of social engineering and digital risks and work to break the paradigms that limit institutional responses.

GASA
Global Anti-Scam Alliance

MATRIX OF RESPONSIBILITIES FOR EFFECTIVE INSTITUTIONAL COORDINATION

Digital security is a shared asset. Attendees agreed that Mexico requires each actor to close specific attack vectors through measurable technical commitments. The following are examples of the types of commitments participants recommended for consideration:

1. Banking & Finance: This sector is well-positioned to lead the implementation of robust anti-fraud systems and appropriate transaction limits. Strategic note: the Mexican Banking Association (ABM) is a key stakeholder and should be a priority attendee at future GASA roundtables and participant in the ongoing process.

2. Telecommunications: Controlling aggregators and call centers, which manage key resources used for scams, should be priority stakeholders for inclusion in the ongoing process. Messaging protocols such as I2P should be addressed, as critical attack vectors that anonymize traffic and create blind spots for traditional operators.

3. Digital platforms: Major tech companies are in a key position to combat the risks posed by bots and Artificial Intelligence. Technological interventions should be explored to identify best practices, e.g. 'Proof of Personhood' layers which work to distinguish humans from AI and reduce the effect of deepfakes on identity verification.

4. Government and regulators: There are opportunities for CNBV, the Security Secretariat and the Foreign Ministry to increase their collaborations to harmonise global governance. Mexico can also leverage its position within the UN Convention on Cybercrime to facilitate cross-border prosecutions and asset recovery.

GASA
Global Anti-Scam Alliance

ROADMAP: IMPLEMENTATION AND QUICK WINS

In order to restore consumer confidence and break the cycle of impunity, a national plan or an anti-fraud and anti-scam public policy agenda should be considered. Organizations such as GASA Mexico are well-positioned to support specific actions within the ecosystem as part of this agenda.

Proposed Implementation Milestones

- ☐ **Global Alignment (March 2025):** Strategic participation in the Vienna Fraud Summit to integrate international standards from the UN and Interpol.
- ☐ **Private Sector Collaboration:** Establishment of a data-sharing protocol between banks and telecoms to track the origin of fraudulent calls and messages without waiting for lengthy legislative cycles.
- ☐ **Restoration of Trust:** Documentation and mass dissemination of successful asset recovery cases, demonstrating that coordinated reporting leads to arrests and the return of funds.

CONCLUSION: TOWARDS A CULTURE OF NATIONAL PREVENTION

The success of specific actions and/or the chosen path will not be measured by the sophistication of the technology used, but by the **restoration of trust in the financial and digital systems**. With 48% of complaints to CONDUSEF relating to fraud, the cost of inaction would be the erosion of the digital economy. While technology and cryptography are essential tools, the foundation of an effective defence is a culture of prevention that permeates from senior government management to the general public.

Mexico must cease to be an attractive market for criminals and transform itself into a highly resilient jurisdiction by taking active responsibility.

"The vision is to establish a true cross-sector dialogue and a national roadmap aimed at identifying an agenda against scams, fraud, and digital deception. This must be a multi-stakeholder strategy built with principal focus on the combination of public and private sector efforts to protect citizens."

Sissi De La Peña
Director – Mexico Chapter, Global Anti-Scam Alliance