EastBayMUN

all suspects are innocent until proven guilty in court of law

INTERPOL

SPECIAL ASSIGNMENT

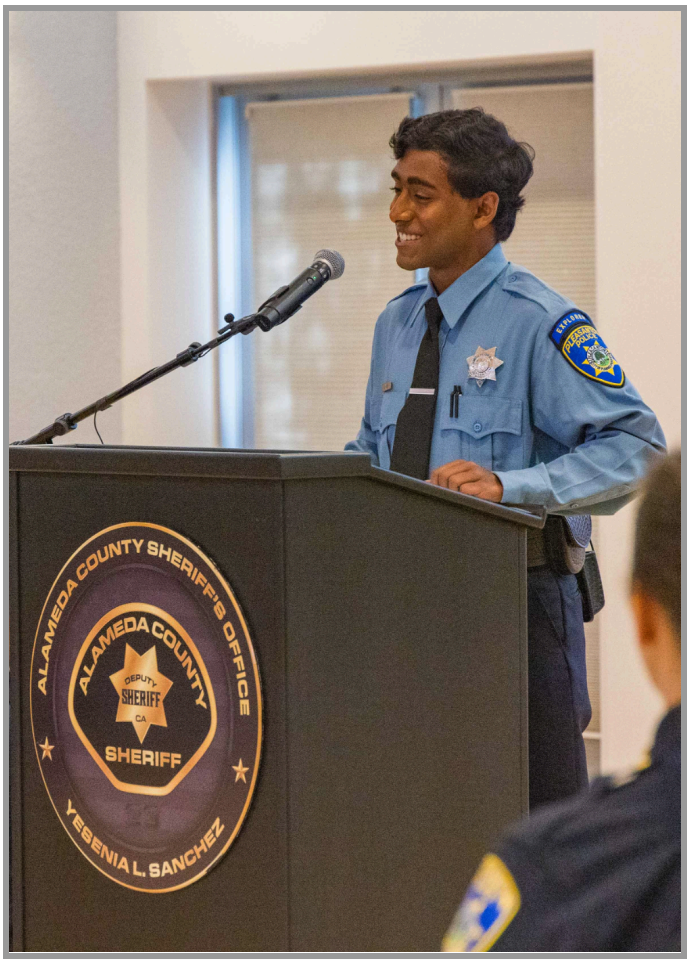
INTERNET FRAUD

Table of Contents

Chair Introductions 2
Committee Overview 4
Topic Background 5
Past International Action 9
Key Issues 11
Questions to Consider 11
Works Cited 12

Chair Introductions

Co-Chair: Dev Arun



Hello Delegates! My name is Dev Arun, and I will be one of your co-chairs of INTERPOL for EBMUN 2025. I'm a senior at Foothill High School, and I've been doing MUN for the past six years. This will be my 40th and last conference.

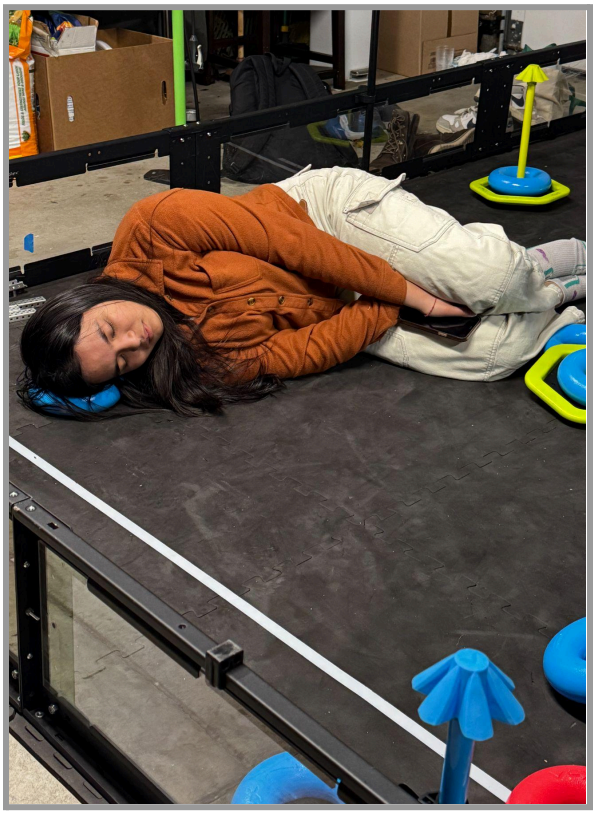
Outside of MUN, I do Track and Field, primarily running the 1600m and 800m. I also volunteer with my local Police Department.

The picture to the right is me speaking to a crowd full of people, including multiple Police Chiefs, as a Class Speaker for the Alameda County Sheriff's Office Explorers Academy. It shows how far MUN can influence you and your life outside of the activity.

I look forward to the engaging debate you will bring to the committee.

Co-Chair: Prisha Sinha

Howdy delegates! My name is Prisha Sinha, and, along with being one of your co-chairs, I am a senior at California High School. I am currently in my fourth year of MUN, and have attended around 15 conferences these past few years. This will be my third and final time chairing a specialized committee, in a topic I find both interesting and comical.



Outside of MUN, you can typically find me building and competing in VEX robotics, gushing over indie folk and hyperpop music artists, or advocating for and researching up-and-coming technology in the field of nuclear energy. If you're interested in anything related to nuclear science, I'm your go-to gal!

Best of luck! If you have any questions or concerns about procedure or on the topic, feel free to email me at prisha.sinha224@gmail.com. Happy researching, I can't wait to see what you all bring to committee!

Committee Overview

The International Criminal Police Organization (INTERPOL) is a global organization of law enforcement agencies. With 196 members, INTERPOL works to secure justice for crime victims worldwide.

While not directly under the United Nations' jurisdiction, the agency frequently works to ensure the smoothest possible operation of law enforcement. This is done through a state-of-the-art data-sharing center, where international police institutions will have access to criminal activity to predict, prevent, and overcome crime.

For EBMUN XI, INTERPOL will operate more actively compared to a typical General Assembly. This means the dias will seek action-based solutions under directives rather than resolutions. We'd be expecting more directives from delegates than GAs, who usually do one in an entire conference weekend. We'd be expecting two or more shorter directives. That also means we'll be receiving updates on how our directives have interacted with the real world. Delegates are expected to come up with solutions to quickly respond to issues to ensure they don't escalate any further.

Topic Background

Since the conception of the Internet in the early 1990s, internet fraud, the deception of users on the Internet through providing and withholding incorrect information to trick victims out of money and other capital, has served as its crux. Siphoning billions of dollars from consumers, these instances of cybercrime have since been established as one of the main concerns of INTERPOL in ensuring international security.

Early cybercrime, namely phishing, mostly only stole user information regarding passwords to online payment systems while using rudimentary algorithms to extract money from victims' bank accounts. However, as these services adopted more substantial modes of security through data encryption (concerning the scrambling of information into data or code), multi-factor authentication (requiring users to take multiple steps to verify their identity), and IP tracking (using the location from which the transaction occurred to judge its likelihood of authenticity), scammers began to exploit the human aspect of these transactions, making it easier for them to override these securities by getting money extracted from the source itself.

These newer scams have taken several forms, including (but not limited to) e-commerce, romance, tech support, and investment and cryptocurrency scams.

E-Commerce Scams

E-commerce scams are instances of fraud where users purchase exceptionally cheap knock-offs of either luxury or everyday items. Although scammers may create their own counterfeit brands, most of these frauds often mimic real brands, while labeling themselves as the original. Victims

of these scams often never receive the items they paid for and instead receive unsafe, low-quality versions of the same product.

Internet users often fall for these scams by clicking on ads that advertise the low price of these false products, redirecting them to a fraudulent website (which may consist of pictures and descriptions stolen from the legitimate seller) where the target makes their payment.

Romance Scams

Although they may take differing forms from each other, romance scams all operate on the same principles, typically on social media and dating apps. Scammers begin by establishing a genuine connection with their victim, creating promises of meeting each other, getting married, and leading a life together in the future. However, none of these dreams are ever realized, and instead, the scammers begin to ask for help in paying for medical emergencies or conducting business ventures. They will later ask for your online bank account information, using it to conduct theft and other fraudulent schemes.

Tech Support Scams

Tech support frauds concern scammers who trick their targets into believing that their computer is facing serious problems, such as a virus. Through creating fake pop-ups of warning messages on certain websites (which typically have URLs that are slightly misspelled, mimicking real websites such as *google.com* or *amazon.com*), these scammers coerce victims to call a number that directs them to a fraudulent tech support agent. This agent then asks for their target to reimburse them for extracting the fake virus from their computer, tricking them out of money. In

some cases, these agents install malware onto their victims' computers (such as remote access tools and keyloggers) to steal banking login details and other personal information.

Investment and Cryptocurrency Scams

These scams, also known as "pig butchering," start similarly to romance frauds, where scammers scout for potential victims on social media and dating apps. After establishing a connection with their target, they introduce them to investing using cryptocurrency. They instruct their target to convert some money in their bank account into cryptocurrency, and to transfer that currency into a fraudulent investment website created by the scammers. The returns on the investment account will look incredibly promising in the beginning, motivating the target to invest more. Although the victim can initially withdraw money from their accounts on the fraudulent website, they will later come across "fees" that disable them from doing so, allowing the scammers to siphon more money from them.

Clearly, these scams take many forms and are incredibly difficult to detect without prior knowledge. In fact, so many people fall victim to them that, according to a 2024 Global Anti-Scam Alliance report, more than one trillion USD was lost to scam calls worldwide, in nations such as Canada, Pakistan, Kenya, Denmark, and many others. Unfortunately, only a measly 4% of reported targets recovered from the losses they incurred. Along with the massive losses in money, however (which, according to the Center for Strategic and International Studies, represented almost 0.8% of the globe's GDP in 2018), other troubling aspects of internet fraud are found in its origin: scam centers.

Scam centers, or fraud hubs, are organizations that carry out the aforementioned scams against internet users. One type of these hubs is known as call centers, which consist of workers from poor areas with low job opportunities (who, oftentimes are in desperate need of the large sums of money they receive through fraud) who work towards scamming people into spending money on fraudulent services, whether it be extracting phony malware off of their computers or getting contracted at a fake job.

However, the more concerning behaviors of these centers concern the ones found in Southeast Asia, which employ human trafficking and modern slavery to force foreign nationals into conducting internet scams. Often run by Chinese crime syndicates in special economic zones or casinos, the traffickers lure their victims into conducting scams by confiscating their passports and threatening them with physical abuse, organ harvesting, and forced prostitution if they choose against executing these scams. They are also prevented from leaving unless they pay an exorbitant sum of money, often amounting to millions in the native currency of the trafficked victim. These scam center workers are trained to create convincing social media and dating personas to tempt their Westerner targets into romance and cryptocurrency scams, and are forced to meet certain quotas by their bosses to prevent abuse.

Despite the lucrative monetary gain, it is clear that these instances of fraud pose a larger net negative due to the international economic losses, along with the gross disregard of human rights. Through improving education and internet security against these scams, along with providing some sort of economic outlet for poor and trafficked scam center workers alike, there is an unmistakable possibility that these abuse of humans and money can be stopped.

Past International Action

INTERPOL has made considerable strides towards ensuring safety against cybercrime. One such movement, known as Operation First Light 2024, was able to recover almost USD 257 million from e-commerce, investment, and romance scams through the freezing of thousands of fraudulent bank accounts internationally. Using INTERPOL's Global Rapid Intervention of Payments (I-GRIP), INTERPOL was able to track down and intercept illegal transfers of money, leading them to intercept numerous fraudulent operations. One highlight of this operation was the dismantling of a crime network in Namibia, where 88 forced workers were saved and hundreds of electronic devices were confiscated for investigation by the INTERPOL General Secretariat. INTERPOL has lead other, similar operations, such as Operation Goldfish Alpha, Operation Night Fury, and the ASEAN and AMERICAS operations to thwart fraudulent websites and malware affecting residential and government devices alike.

Additionally, INTERPOL has created several Joint Operations with its member countries (specifically in Africa and Asia) to conduct more specific crackdowns on cybercrime syndicates in their respective areas. By providing said member countries with the means to gather and analyze cybercrime data, INTERPOL is able to arm countries with the disrupt and take coordinated action against internet fraud. Along with these Joint Operations, INTERPOL has developed "assessments" (such as the Financial Fraud assessment) to evaluate how technology may be impacting cybercrime, and what types of fraudulent internet scams are most prevalent. These assessments also judge what actions need to be taken against these cons to prevent them.

Finally, INTERPOL has also taken part in educational campaigns to improve internet safety. The Think Twice campaign, which includes a series of short videos to inform internet users of potential scams, while urging the use of safety features such as in-person and two-factor authentication, along with coercing them to be more skeptical of content they come across online. Think Twice dissects the top threats identified by INTERPOL and its member countries concerning internet safety, allowing for users to develop caution in the most critical areas.

Key Issues

Delegates should aim to tackle all aspects of internet fraud. This should include improving online security through the development of cybersecure technology, along with developing means to inform more internet users on how to detect and react to such scams in their day-to-day lives. Additionally, delegates should also attempt to thwart human trafficking and modern slavery operations that stem from conducting cybercrime. This should result in a multi-faceted and detailed solution to improve internet safety internationally.

Questions to Consider

1. What types of scams should INTERPOL aim to thwart?
2. What incentivizes people to work for scam agencies? How can this be mitigated?
3. What are targets of scams unaware of when falling victim to them? How can these risks be avoided?
4. What should public awareness campaigns against cybercrime look like? How can they be made accessible to everyone?
5. What type of technology can INTERPOL use to improve their crackdown operations?
6. How can international cooperation be utilized to help bolster crackdowns? How can transparency between government officials be incentivized?
7. How does government corruption play a role in cybercrime? Can this be evaded?
8. How can INTERPOL collaborate with the private sector to improve internet safety?
9. How do fraudulent schemes impact the global economy?
10. How can the development of scams due to improving technology be anticipated and counteracted by governments?

Works Cited

"$257 Million Seized in Global Police Crackdown Against Online Scams." *INTERPOL*, 2024, https://www.interpol.int/en/News-and-Events/News/2024/USD-257-million-seized-in-global-police-crackdown-against-online-scams.

"The Global State of Scams Report 2024: $1 Trillion Stolen in 12 Months." *Global Anti-Scam Alliance (GASA)*, 2024, https://www.gasa.org/post/global-state-of-scams-report-2024-1-trillion-stolen-in-12-months-gasa-feedzai.

"How Myanmar Became a Global Center for Cyber Scams." *Council on Foreign Relations (CFR)*, https://www.cfr.org/in-brief/how-myanmar-became-global-center-cyber-scams.

"Indian Scam Call Centres Looted Over $10 Billion in 11 Months from US Senior Citizens This Year." *Firstpost*, https://www.firstpost.com/tech/news-analysis/indian-scam-call-centres-looted-over-10-billion-in-11-months-from-us-senior-citizens-this-year-11896001.html.

"INTERPOL Campaign Warns Against Cyber and Financial Crimes." *INTERPOL*, 2024, https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-campaign-warns-against-cyber-and-financial-crimes.

"INTERPOL Financial Fraud Assessment: A Global Threat Boosted by Technology." *INTERPOL*, 2024, https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-Financial-Fraud-assessment-A-global-threat-boosted-by-technology.

"Internet Fraud." *Wikipedia*, https://en.wikipedia.org/wiki/Internet_fraud.

"National Crimes and Victim Resources: Cryptocurrency Investment Fraud." *FBI*, https://www.fbi.gov/how-we-can-help-you/victim-services/national-crimes-and-victim-resources/cryptocurrency-investment-fraud.

"Phishing's America Online Origins." *Phishing.org*, https://www.phishing.org/history-of-phishing#:~:text=Phishing's%20America%20Online%20Origins.

"Ringing in Our Fears 2024." *PIRG*, 2024, https://pirg.org/edfund/resources/ringing-in-our-fears-2024/.

"Romance Scams." *FBI*, https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/romance-scams.

"Scam Center." *Wikipedia*, https://en.wikipedia.org/wiki/Scam_center.

Stripe. "Types of Ecommerce Fraud." *Stripe*, https://stripe.com/resources/more/types-of-ecommerce-fraud#:~:text=Chargeback%20fraud.

"The History and Evolution of Fraud." *Fraud.com*, https://www.fraud.com/post/the-history-and-evolution-of-fraud.

"The What, How, and Dangers of Tech Support Scams." *Federal Trade Commission (FTC)*, https://consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams.

"What Is INTERPOL?" *INTERPOL*, https://www.interpol.int/en/Who-we-are/What-is-INTERPOL.

"What to Know About Cryptocurrency and Scams." *Federal Trade Commission (FTC)*, https://consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams.