

Case 37

Contributor: Agenfor International

Assessed case number: United States v. Garcia, No. 3:19-cr-04488-JLS (S.D. Cal. Nov. 6, 2019)

Title: Threat of the use of force or of other forms of coercion, pornography industry

- What type of trafficking/exploitation is being analysed?**

Sexual THB	Forced Labour	Forced Criminal Activities	Minor Exploitation and forced adoption	Polycrime	Other (Specify the type)	All the aforementioned
X						

- Please provide a brief description of the case (about 500 words)**

The defendant, Ruben Andre Garcia, has engaged in coercion, force and fraud to sexual exploit women with commercial acts. Between 2013 and 2019, he recruited young women to participate in commercial sex act videos, which were later posted on pornography websites, GirlsDoPorn (GDP), GirlsDoToys (GDT), and PornHub, without the women’s consent. He convinced the women usually stating that the material would not be posted online or be broadcasted within the U.S. or that it is not possible for someone who they knew to see the content.

Several other co-conspirators (Michael James Pratt, Matthew Isaac Wolfe, Theodore Wilfred Gyi, Valorie Moser, and others) participated in the sex trafficking conspiracy. The defendant, and a co-conspirator (Pratt), which also aided and abbetted in the recruitment of women, posted fake advertisements on Craigslist(an online advertisement website) for modelling jobs. In order to convince the victims who contacted the advertisement, all the defentants hired another women upon a fee, and if the victim agreed to be filmed, they made sure to further convince her by saying that the material would not be broadcasted online. Even though the victims complained because of painful sexual acts, the defendants continued filming in most situations through coercion, threat and force.



- Which is the *modus operandi* of the entities using cyber tools for trafficking and/or exploitation?

MODUS OPERANDI	Yes/No	Description
Internet: Pornography Websites and Craigslist (an online advertisement website)	Yes	The defendants used pornography websites to disseminate the explicit content, without the women’s consent. Furthermore, they placed fake advertisements through Craigslist to lure women into thinking that they will be doing modelling jobs.
Other		

- Please provide more details on the perpetrator(s):

Was/were the perpetrator(s) male or female?	Male
Which is the nationality of the perpetrator(s)?	American
In which country was he/she, were they operating?	America
Was it an individual or a group?	A group
Were there any preliminary indicators for early detection?	No
Which other aspects are important?	

- Which were the main characteristics of the victim(s)?

THB Victims	Involved (x)	Please describe in more detail
Men		
Women	X	
Minors		
LGTBI		
Country of origin	X	American
Country of exploitation	X	America
Capturing Method		
Coercion Method (debt-bonded, victims’ families threatened...)	X	d were frequently threatened with lawsuits and the posting of their videos online, the cancelation of tickets for their flights home, and the blocking of the victims’ exit from the hotel rooms with equipment where they were filming the videos to make the women feel that they could not leave.



Handing over the passport		
Other		
Unknown		

• **What were the money laundering mechanisms used by traffickers?**

Money Laundering Mechanisms	Involved (x)	Please describe in more detail
Checks and money orders to anonymous post office boxes		
Back accounts in foreign countries		
Funnel account(s)		
Route cash from different cities		
Money Mules		
Hawala System		
Purchase of corporate vehicles or real estate		
Cash business entities such as restaurants or bars		
Other		
Unknown	X	

• **Has the case been tried or is it still under investigation?**

Legal Procedure	Yes/No	Please describe in more detail
Case with judgment	Yes	The primary defendant was found guilty of sex trafficking by force, fraud and coercion and sentenced to 20 years of imprisonment, while to other co-conspirators are still fugitive.
Under investigation	No	

• **What was the economic evidence of the crime?**

Economic evidence	Yes/No	Please describe in more detail
Money Transfers		
Banks Accounts		
Unjustified Financial Wealth		
Network Accountancy		
Financial Study of the Victim		
Wallet Cards		
Suspicious transactions		
Cryptocurrency exchanges or		



payments		
Cash payments		
Faster Payments Inwards (FPI) from the same entity		
Same mobile number or email address		
Hawala Payments		
Various bank accounts beneficiaries		
Others		
Unknown	X	

• **What activities in internet were considered suspicious?**

Internet Activities	Yes/No	Please describe in more detail
money transfers	No	
Purchases at online gaming sites	No	
Ads on Backpage.com or similar sites	No	
Social media to recruitment	No	
Use of digital platforms to advertise deceptive job offers and to market exploitative services to potential paying customers	No	
Fishing potential victims by posting advertisements	Yes	The victims were deceived into thinking that they will be hired possibly into modelling jobs, through fake advertisements made in Craigslist.
Use of video equipment to stream and broadcast exploitative services	Yes	The recorded pornographic material were distributed later without the women's consent, in pornographic websites.
Used of multiple online profiles	No	
Use of specific apps: Please circle the relevant apps or add the name at the end if not listed	No	Ex: 1) For Advertising: Facebook, Instagram, TikTok, etc.; 2) For Recruitment and Communication: FaceTime, IMO, Messenger, Signal, Signal, Skype, Viber, WA, WeChat, Zalo, etc. 3) For Logistic: video-sharing platforms distributing essential logistic instructions, satellite images and photos, planned routes, Google Maps waypoints, GPS data, etc.; Guidance, including mapping applications (Maps.me, Google Maps) for remotely guiding migrants across borders through tailor-made tutorials and YouTube videos containing detailed guides on how to navigate migrant routes, where to cross borders or buy fake documents,



		<p>how to find smuggling hotspots, shelter or assistance, etc.;</p> <p>4) For Payments, online transfer of fees and documentation of payment proof via messaging services, hawala, etc.</p> <p>5) Countermeasures adopted by smugglers to anonymize their services, AppLocks, Secure Folders, burner applications, DiskDigger, private VPN connections, or clone apps, Fake GPS and modified display caller ID (Numberbook).</p> <p>6) Other:</p>
Others	No	

• **Other relevant information or important case specificities:**

		Please describe in more detail

