Cyrus R. Vance, Jr.
New York County District Attorney

January 30, 2018

Good afternoon, Representative Wagner and members of the House Financial Services Committee's Subcommittee on Oversight and Investigations. I am New York County District Attorney Cyrus R. Vance, Jr. Thank you for the opportunity today to discuss the shifting economic aspects and implications of human trafficking.

The nature of human trafficking in Manhattan, the United States, and around the globe has transformed dramatically in the 21st century. The illicit transactions that have historically comprised the backbone of this economy are no longer confined to street corners. Today, advances in technology and finance have pushed human trafficking online, hidden and protected by cryptocurrency, laundered money, foreign internet servers, and anonymous messaging applications.

As a result, those who investigate and prosecute these crimes have been forced to play catch-up with traffickers who are increasingly skilled and evasive. In 2014, my Office announced the creation of our Human Trafficking Response Unit. Tasked with tackling an incredibly complex issue, the Unit is housed within our Special Victims Bureau and has a dedicated social worker to address the needs of severely traumatized victims. However, in addition to addressing the violent nature of trafficking, the Unit also recognizes the necessity of focusing on the intricate financial and technological aspects of this crime. To this end, the

Unit employs a forensic accountant and a data engineer to develop new approaches to emerging issues, such as tracing money movement across industries and jurisdictions, identifying the online footprints of sex trafficking operations, and using innovative technologies to proactively screen cases and the online market for commercial sex for signs of human trafficking. We are also one of the first prosecutor's office in the country to use a ground-breaking search tool called Memex, a technology that extends beyond the reach of commercial search engines into the "dark" or "deep web." Created by the U.S. Department of Defense's Defense Advanced Research Projects Agency (DARPA), Memex's suite of tools quickly and thoroughly organizes intelligence from online prostitution advertisements to aid human trafficking investigations and prosecutions. Memex is now used in every human trafficking investigation and prosecution brought by my Office. Last year, we screened more than 6,000 arrests for signs of human trafficking using Memex tools. We also used Memex in 271 human trafficking investigations and in six new sex trafficking indictments that were brought in 2017.

Currently, a significant portion of the human trafficking economy exists online. In December 2017, more than 7,000 prostitution advertisements were posted on Backpage.com for Manhattan alone. Over the past decade, tens of thousands of clients have posted crass and detailed reviews of prostitution encounters on The Erotic Review. But trafficking's online presence extends far beyond just Backpage and The Erotic Review. On the supply side, the list includes Craigslist, Cityvibe, ECCIE Worldwide, and Escorts In College, in addition to smaller independent operations that conduct business on websites hosted by GoDaddy, Wix, and Squarespace. On the demand side, clients use websites like UtopiaGuide and Spa Hunters to identify and discuss services, even going so far as to leave reviews on sites like Yelp.

Financially, the human trafficking economy is just as expansive and intricate. Traffickers employ sophisticated techniques to move money rapidly and conceal it efficiently. Moving beyond traditional methods such as wire transfers, traffickers have turned to companies including money service providers to arrange transportation for their victims, pay members of their operations, and move their ill-gotten gains abroad to countries like Russia and China in the blink of an eye. Traffickers also commonly launder money by opening multiple business accounts at different banks, as well as transferring checks and cash between accounts to cover their tracks. In many cases, tens of thousands of dollars have already been moved before investigators even have a chance to review bank records.

But not all financial techniques are so extensive. As more and more banks and credit card companies refuse to do business with those who knowingly facilitate sex trafficking, criminals have turned to prepaid gift cards, which essentially function as credit cards while enabling the traffickers to maintain anonymity. These cards can be used to register websites, obtain cryptocurrency, and even purchase sex. In one Manhattan District Attorney's Office investigation, a Visa Vanilla card was used to register an escort website on GoDaddy, allowing the operator to remain nameless.

Another consequential shift we have witnessed in our investigations has been the rise of cryptocurrency. In most cases, we do not see traffickers accepting cryptocurrencies from buyers of sex. Instead, the most significant impact of these currencies in sex trafficking investigations has been their role in the online economy. They are used both by traffickers to purchase advertisements and by sex buyers to purchase premium memberships on review board websites. The volume of advertisements and memberships, alongside the drastic increase in the value of digital currencies such as Bitcoin, has caused the profits of those who operate websites that facilitate both the supply and demand side of the economy to

skyrocket. Over the last year, the increase in the value of Bitcoin has generated several million dollars in profit for one popular review site.

This trend is, of course, driven by the fact that mainstream credit card companies such as Visa and MasterCard have refused to do business with Backpage. Therefore, without cryptocurrencies, the site would be relegated to using unreliable processors as a last resort. These processors charge steep fees – sometimes 30 to 40 percent of the transaction amount – to process transactions, thereby decreasing the site's profits.

Also of note, some members of the cryptocurrency community appear to cater to traffickers who are trying to post advertisements on Backpage and other sites. Paxful, a peer-to-peer marketplace where users can exchange gift cards for Bitcoin, explicitly publishes YouTube videos laying out step-by-step instructions for turning these cards into cryptocurrencies to pay for Backpage ads. One such video can be found here: https://www.youtube.com/watch?v=5o2T4DF0iSA.

There is no question that the technological and financial environment that I have described presents challenges for investigators and prosecutors. However, the Manhattan District Attorney's Office is taking several steps to address these critical issues. First, in 2013, we formed a working group with the Thomson Reuters Foundation, several banking institutions, and leading anti-trafficking NGOs aimed at helping the wider industry to identify and report irregularities in financial transactions that might be linked to human trafficking activity. We are a member of the North America Banks Alliance, a partnership between financial institutions, non-profit organizations, and law enforcement coordinated by the Thomson Reuters Foundation. This organization seeks to develop strategies and best practices around the economic aspects of human trafficking.

Second, we have developed relationships with banks like JP Morgan Chase and Bank of America, working with their compliance and internal investigation teams to proactively seek out trafficking indicators. Relationships with such institutions allow our analysts to quickly target and investigate potentially illicit financial activity. Lastly, we collaborate with money services providers to create preemptive alerts on target accounts and aliases so that our investigators can intercept and identify those individuals when they send or receive money.

Despite these positive developments, several roadblocks have the potential to impede human trafficking investigations. One of these roadblocks is the emergence of encrypted communications technologies, including WeChat, WhatsApp, and Viber. These applications allow users to communicate over the internet, as opposed to traditional telecommunications networks. On the ground, this means that traffickers can communicate in complete privacy. The companies themselves are also not required to maintain call records or text content. As a result, it is impossible to view or obtain these records without physically seizing the device. Further, a number of these companies are headquartered abroad, such as the Chinese company WeChat or the Canadian company TextNow, which prevents my Office from receiving vital support and cooperation from their compliance departments.

In addition to encrypted applications, a significant challenge we encounter is that the smartphones themselves are often encrypted. This a topic that I have testified about several times before Congress because it has had an enormously negative impact on the ability of law enforcement to do our jobs. Since 2014, Apple and Google have engineered their mobile devices so that law enforcement cannot access critical evidence on those devices, even with a court order. Criminals – including human traffickers – know that smartphones now enable them to communicate with impunity about their crimes. In a real example from a case

involving Promoting Prostitution charges prosecuted by my Office, an incarcerated defendant tells his friend on a lawfully recorded landline phone from jail, "Apple and Google came out with these softwares [sic] that I can no longer be [un]encrypted by the police… [i]f our phone[s are] running on iOS8 software, they can't open my phone. This may be [a]nother gift from God." That is not a gift from God, but an unintended gift from two of the largest technology companies in the world. In the investigation against this defendant, there was evidence that he engaged in force, fraud, and coercion during his operation, and a search warrant was issued authorizing a search of his device. He spoke repeatedly of how much evidence was on his phone, stating that the government was trying to get higher charges on him and there was evidence on the phone. However, without access to his encrypted phone, we could not bring sex trafficking charges. Instead, the top charge we were able to bring was a much less serious crime, Promoting Prostitution in the Third Degree, to which he pleaded guilty.

Our human trafficking investigations are also hindered by delayed search warrant and subpoena returns. As the trafficking economy shifts to an instantaneous online environment, it has become increasingly critical that prosecutors receive records in a timely manner to avoid falling behind in investigations. Although many companies, such as Verizon and AT&T, are quick to respond, there are many more that routinely fail to provide records within a reasonable timeframe. And while I certainly recognize the voluminous workload that these companies face, overly lengthy delays are simply unacceptable. For instance, some companies—including GoDaddy and T-Mobile—take as long as six months to provide records, while others—including Craigslist—take even longer. In cases of human trafficking, six months can feel like an eternity to victims of sexual violence and coercion. Further, certain companies like Airbnb will not comply with subpoenas that include legal

nondisclosure orders unless the length of nondisclosure is enumerated. In a recent case, Airbnb informed my Office that it would not comply with a subpoena unless that period of nondisclosure was 90 days or fewer. Some of the more complex human trafficking investigations can take much longer than that. Thus, disclosing the existence of subpoenas after 90 days threatens to compromise long-term investigations, thereby invalidating the hard work of our investigators, analysts, and prosecutors.

Another challenge we face in our human trafficking cases is obtaining data from outside the United States, particularly because many data servers that contain critical evidence of trafficking reside in other countries. Mutual legal assistance treaties (MLATs), which are agreements between countries that create obligations to assist one another with criminal investigations, have struggled to keep pace with the complexity of data transfers across foreign jurisdictions. The MLAT process is outdated and not compatible with the way financial transactions occur in the modern age. For example, while money can be moved through various countries at the speed of a computer, it takes us many months – if at all – to obtain documents regarding that money movement when we must go through the MLAT process. One of the problems is that MLATs require full administrative legal processes in each country involved, and even MLATs between countries with existing special relationships can be byzantine, dramatically slowing down the transfer of important information. Consequently, by the time we eventually get the evidence, a case may no longer be prosecutable, or the harm caused to victims is no longer reparable.

Finally, obtaining data on financial transactions can be challenging because our country's lax incorporation laws make it easy for criminals to hide money behind anonymous shell companies and launder it through U. S. and foreign banks and their branches. It is almost a certainty that, at this very moment, a human trafficker, terrorist cell, drug cartel, or

corrupt government official is using an anonymous U.S. shell corporation to finance illicit activities. On a near-daily basis we encounter a company or network of companies involved in suspicious activity, but we are unable to glean who is actually controlling and benefiting from those entities, and from their illicit activity. In other words, we cannot identify the criminal because the criminal has used layers of shell companies to frustrate investigators and protect himself from prosecution.

It is clear that our laws must keep pace with these rapid changes in both finance and technology. To fail to do so would leave law enforcement trailing behind sophisticated criminals who seek to operate anonymously beyond the existing legal framework. But we must remember that, behind these walls of encryption, laundering, and anonymity, there exist trafficked victims living in fear of force, fraud, and coercion. Traffickers seek to exploit the vulnerable without consequence, and our laws must not facilitate their ability to do so.

Thank you. I am happy to take your questions.