Illicit Trade in the United States Postal Service

By Candice Wilson

Introduction

E-commerce, coupled with free trade and global communications, has ignited an enormous use of the United States Postal Service (USPS). Inbound international mail alone is at hundreds of millions of pieces each year. Illicit goods sent through the mail are causing a significant national security and health issue. Anyone can order fentanyl from China or Mexico or counterfeit Percocet and have it delivered to their front door virtually unchecked. These goods have created a national health emergency from counterfeit personal protective equipment (PPE) and wildlife trafficking, counterfeit medication to illicit narcotics. The criminal proceeds from these illegal trades fund terrorist groups and their terror attacks globally and transnational organized crime groups (TOC) that influence and often capture weak nations.

Now more than ever, it is crucial to drastically enhance the efficacy of the USPS targeting procedures of suspicious parcels. This paper will discuss which entities are responsible for mail inspection, both domestic and international, and techniques and technology USPS analysts and inspectors use to target suspicious parcels.

This paper will also discuss the unique range of illegal goods sent in the mail. Discussing the typology of illicit goods is critical, as it naturally bridges the discussion into the convergence of unlawful items and criminal groups. Possessing the intelligence of converged goods provides investigators with the ability to target choke points that will help dismantle

criminal groups by arresting super facilitators and simultaneously reducing the number of targets that often overwhelms law enforcement.

Last, exploring policy, civic and industry response to illicit trade, and technology is necessary because data-driven, evidence-based technology and intelligence can assist with investigations. Further, engagement by all involved places a needful spotlight on officials, legitimate corporations, and individuals who intentionally or unwittingly enable illicit trade with little to no consequence. It is unsettling to think about the billions spent securing our physical borders. Yet, the USPS other private mail services have lagged behind far too long to keep illegal and dangerous products from entering the United States, despite their genuine and best efforts by some, which border officials and postal inspectors are working hard to detect and confiscate. The failure of the USPS runs entirely counterproductive to our national security efforts.

Parcel Interdiction: Procedure, Techniques and Technology

The USPS coordinates with multiple entities to ensure the safety of parcels within and entering our borders. Starting at the international level, the Universal Postal Union (UPU), a specialized unit within the United Nations, is the epicenter for international cooperation on postal issues, including mail security. Its existence is why countries can send mail across the globe without separate bilateral agreements with each country. The UPU holds significant leverage, as it can suspend its members, including the USPS, if requirements go unfulfilled as mandated by the federal government (Marchand & Kosar, 2021). Requirements include the new federal mandates stemming from the Synthetics Trafficking & Overdose Prevention (STOP) Act.

In 2018, the STOP act became law. One of the key elements of this act requires advanced electronic data (AED) on all inbound international parcels, such as names, origin, weight, and contents information. Officials will deny entry of any package without an AED barcode, per the federal mandate (Porter, 2020). Once international packages arrive, the first stop is at the International Service Centers (ISC) located in San Francisco, New York, Miami, Los Angeles, and Chicago, where the parcels are subject to inspection by the Customs and Border Protection (CBP).

With the STOP Act in place, the USPS and the CBP reject packages with no AED information. The AED information initially comes from foreign post offices (F.P.O.) of nations that have agreed to, or are capable of, providing this data (Combating the Opioid Crisis, 2020). In addition to the STOP Act, other mandates exist that authorize investigators to inspect suspicious parcels. The Code of Federal Regulations (C.F.R.), 39 CFR 233.11, pertains to screening mail transported by aircraft. This code authorizes, along with 39 U.S.C. 5401, the Postal Service the power to screen a suspicious parcel they feel may pose an immediate threat (bomb, explosives, or firearms) without a search warrant or the sender and recipients' consent and can do so without opening the package. If the screening determines the parcel is a threat, the package can be opened and processed to eliminate this threat (Federal Register, 2021).

However, there is a concern regarding the STOP Act and the waivers granted to certain countries. Over 130 countries granted waivers which signify they do not have to comply with the STOP Act requirements. In other words, 130 countries do not have to provide accurate sender information, declaration of contents, weight, etc. These are pivotal data points for parcel interdiction analysis and general criminal investigations. This presents a tremendous

vulnerability as illicit groups learn of these waivers and shift their illegal parcel shipments to these countries. Senators Portman and Klobuchar expressed this concern to the United States Post Office and Department of Homeland Security (HSGAC, 2021).

Waivers are granted a waiver if they meet the following three requirements:

1. The country does not have the capacity to collect and transmit AED
2. The country is considered low risk for parcel law and regulations violations.
3. The country has low volumes of parcels as such the parcels can be screened effectively through other means.

Senators Portman and Klobuchar strongly suggested these waivers be temporary and urged the State Department to resolutely work with the UPS and the World Customs Organization to advance global requirements for AED capabilities (HSGAC, 2021).

Once the package is accepted, postal employees utilize a variety of technological options, as illicit contents vary, and one technological option is not a blanket solution for all suspicious parcels. The F.D.A. has supplied postal inspectors with handheld surface-enhanced Raman scattering (SERS) devices to detect opioids and other illicit narcotics (Kimani, Lanzarotta, and Batson, 2021). Other high-tech analyzers help the USPS field divisions scan for illegal drugs and test over 300 illicit substances inside concealed parcels (USPIS, 2021).

In June of 2021, the USPS awarded a $14 million contract to RedWave Technology, purchasing additional portable infrared spectrometers that detect dangerous materials such as drugs, explosives, powders, liquids, and gases (Postal Times, 2021). Postal employees have access to portable x-ray scanners that visualize the contents to detect numerous illicit substances and hazardous materials. Highly trained postal inspectors can recognize signs of a potentially dangerous parcel by examining a parcel's exterior. Inspectors look for clues such as

misspellings of the sender or recipient's handwritten label, excessive use of tape, overuse of stamps to avoid metered postage, the recipient label reads a title only (not addressed to a specific individual), and discoloration or crystallization on the wrapper (USPS, 2019).

The Environmental Protection Agency (E.P.A.) and the Fish and Wildlife Services (FWS) play an essential role in parcel security. As a result of the anthrax scare in 2001, the USPS, E.P.A., Federal Bureau of Investigation (FBI), and public health experts, initiated an irradiation process for parcels addressed to governmental agencies. The mail passes through ionizing radiation in the form of a high-energy beam which kills harmful bacteria like anthrax (E.P.A., 2021). The United States Department of Agriculture advised a list of plants, plant products, and animals to be subject to inspection by the Fish and Wildlife Services. Officials will seize a package and inspect further if one of three criteria exist; the package displays a written declaration the parcel contains an item on this list, the contents are visible, or the package shows signs of odor, stains, dampness, or swarming insects. A USPS inspector may open a package either by consent or a federal search warrant. Besides the USPS, all other mail carriers do not require consent or a warrant to open and inspect a suspicious parcel (USPS, 2014).

Typology of Illicit Goods

New ways of delivering illicit goods include using the USPS, primarily due to the rise in e-commerce and its anonymity. Law enforcement agencies report a significant increase in the use of the postal system, which severely impacts their screening and interdiction capabilities (OECD, 2018). The CBP screens approximately 1 million packages a day at John F. Kennedy International airport, one of nine international mail facilities, looking for illicit food, wildlife, drugs, and illicit proceeds from drugs sales and counterfeit goods. JFK is the largest mail facility

in the nation and handles approximately 60% of all international packages (Narishkin & Cameron, 2021).

The OECD conducted a survey and found counterfeit products and narcotics were the most seized products in Europe and the United States while law enforcement's weapons and illicit tobacco seizures were the next highest. After tobacco and weapons were illegal wildlife products and illegal alcohol (OECD, 2018). According to Narishkin and Cameron's article, counterfeit goods, including the theft of intellectual property rights (IPR), are a trillion-dollar industry and linked to terrorist groups worldwide. In 2018 alone, Customs and Border Patrol seized over 1,800 IPR parcels. If these goods were sold at the standard retail price, the estimated illicit proceeds from these sales would be an estimated $54 million. Customs and postal officials experience the creativeness of drug smugglers when they locate illegal narcotics in Play-Doh cans and children's books, providing a few examples among hundreds of concealment methods. Inspectors also find counterfeit goods such as fake Air Jordan's, Gucci purses, Personal Protection Equipment, Rolex watches (Narishkin & Cameron, 2021).

According to a study published in *Global Crime*, 94% of illegal wildlife seized in the United States belongs to six groups: mammals, reptiles, mollusks, birds, fish, and coral. More than half of the seizures fell into the mammals and reptile groups. The leading means of transportation into the United States were via air cargo intercepted at postal offices by the Fish and Wildlife Services and customs officials. More than 200 thousand specimens were seized from shipments made through the mail. The study found the principal offender was China and their illicit e-commerce activity via social media platforms. (Petrossian, Pires, & van Uhm, 2016).

In January of 2020, China implemented a temporary ban on wildlife trade because of the COVID-19 global pandemic as it is suspected to have originated from trafficking animals. In the first month of the ban, e-commerce platforms and other conservation groups collaborated and removed, deleted, or blocked an estimated 140,000 wildlife products and closed approximately 17,000 accounts revealing how prevalent the online trade of wildlife is in China (Standaert, 2020)

Criminal groups seized the opportunity to send counterfeit medicine claiming to cure COVID or curb the symptoms of the virus, fraudulent test kits, and masks. In March of 2020, at the International Mail Facility (IMF) in Los Angeles, California, the CBP seized fraudulent test kits mailed from the United Kingdom. Inside the parcel were six plastic bags containing vials labeled "Corona Virus 2019nconv (COVID-19)" and "Virus1 Test Kit". The external parcel wrapping read the words "Purified Water Vials," which was flagged by customs officials, which, as previously discussed, suspicious parcel identification in action (USCBP, 2020).

Investigations to Dismantle Illicit Networks Using the USPS

Seizing parcels containing illicit goods often provides insight into where the contraband originated, transited, and destination location. In addition, parcel labels often provide sender and recipient information, including names and addresses. However, the sender's information on illicit parcels is often fraudulent, as the post office does not check identification when the sender mails a package. Each seizure incident can provide critical data on the entire trafficking chain. To allocate law enforcement resources efficiently, information regarding concealment tactics, the nation-states allowing these parcels to pass or incapable of detection, age, gender, and nationality of those participating in the shipment must be collected and analyzed to prevent contraband flows (World WISE, 2016) successfully.

Research reveals the lack of sender information is one of the key reasons illicit trade through postal services thrives domestically, and international bodies are discussing the same issue. The United States Department of State and the Bureau of International Narcotics and Law Enforcement Affairs (INL) met with Malaysia's leading postal service provider, Pos Malaysia, regarding interdiction best practices of illicit goods, especially wildlife trafficking. During discussions, participants discussed interdiction methods and other challenges and made a special mention about the lack of sender information where the mail is first accepted (TRAFFIC, 2020).

Analysts and agents working within the Contraband Interdiction and Investigations (CI2) team is an internal multi-disciplinary unit of subject matter experts, focused on domestic and international narcotics trafficking, provides advanced data analytics for the field investigators (Barksdale, 2019). These analytic capabilities allow intelligence analysts to identify criminal networks or drug trafficking organizations (DTO) through parcel labels, IP data, USPS business records, and other commercial and law enforcement databases.

Sifting through vast amounts of data, especially when investigating social media, may have been a significant issue if not for algorithms. Algorithms sift through millions of posts looking at common drug terms and other classifiers such as photos, behavior, texts, timelines, and other key markers. Once it is determined it may be a dealer account, it is passed on to investigators to investigate further (O'Neill, 2021). Algorithms employing social network analysis for money laundering detection are another valuable tool to detect bad actors in a criminal network and detect accounts associated with the same person. Algorithms that utilize frequent pattern mining and role-finding algorithms within criminal networks are proven to be

effective techniques in money laundering detection and criminal network research (Drezewski, Sepielak, & Filipkowski, 2015).

Supplying a highly targeted intelligence product includes financial information, point of vulnerability (active warrants), social media intelligence, locations, vehicles, mobile phone analysis, and deconfliction with other law enforcement agencies often providing additional intelligence. In other words, resources are not stove-piped, providing investigators with a more comprehensive depiction of the network.

Analysts and investigators working within the United States must create a synergy between each other and international law enforcement bodies to assist with refining the target (Joint Chiefs of Staff, 2016). Interconnectivity absolutely must exist, given the nature of global trade. Evolving from traditional investigation methods, focusing on super fixers or super facilitators, who tend to operate internationally and are often officials within governments, is more effective regarding dismantling their networks. These co-conspirators operate at the intersection of other criminal networks and often possess the skill and resources to allow an illicit network to run. If identified and captured, the effects on the criminal organization, and the additional intelligence seized as a result, far outweigh the arrest of a simple foot soldier, providing very little actionable intelligence (Perlmutter, 2020).

Threat networks are fluid, often-times sophisticated, and work clandestinely. In some instances, threat networks are not entirely clandestine, they operate in plain view. Criminal groups participating in illicit trade have relationships with individuals and public officials working under the cloak of legitimate professions. As Angel Nguyen Swift (2020) stated in her testimony to the House Committee on Financial Services, third-party facilitators such as

attorneys, accountants, and real estate agents enable and actively participate in illegal activity with impunity. Given this fact, financial investigations must be conducted alongside the more traditional criminal investigation of whatever illicit item was seized inside the parcels: drugs, weapons, or any other illegal shipment.

Gretchen Peters, the Executive Director at the Center on Illicit Networks and Transnational Organized Crime, testified to the Subcommittee on National Security that criminal organizations have not moved institutionally to blockchain currency (Peters, 2020). However, obtaining financial transactions to demonstrate money laundering and identify additional co-conspirators is critical. Bad actors have more options to transfer money, whether online, peer-to-peer electronic wire transfers from money services businesses (MSB), mobile cash applications, or cryptocurrencies. The many options available and their anonymity are principal reasons why illicit trade has dramatically increased.

The USPS utilizes undercover cryptocurrency accounts via the USPIS Cryptocurrency Fund Program to purchase illicit goods, mainly narcotics (USPSOIG, 2021). The investigator can identify cryptocurrency accounts to seize due to their investigation by notifying the Asset Forfeiture Unit (AFU) and transferring the seizure to AFU's wallet. The AFU transfers funds to the United States Marshals Service for disposal, where the US Marshals Service ultimately returns the proceeds of sale to the USPIS (USPISOIG, 2021). In 2019, the USPIS seized $24 million in illicit proceeds of various forms, including cryptocurrency (USPS, 2020).

Cryptocurrency is used on the surface web as well as the Dark Web. A joint investigation involving the USPIS, and DEA identified and arrested a Dark Web vendor Alaa Awalli aka "Dopeboy210," for the distribution of fentanyl, cocaine, and methamphetamine online and in

the San Antonio and Houston, Texas area. USPS Inspectors initially located an Easy Post account used by Awalli. Through the parcel history of this Easy Post account, they learned that this vendor was the source of supply for other Dark Web vendors. Officials estimate Awalli distributed approximately 895,000 pills, mostly oxycodone pills pressed with fentanyl, methamphetamine-laced Adderall, and Xanax. Awalli was sentenced to 30 years in federal prison (USPS, 2020). Officials believe the fentanyl and the commercial pill press used to manufacture the pills were shipped from China. The enormity of this illegal operation was discovered when officials recovered 120 packages of pills ready to be delivered and 70 parcels already mailed but intercepted by the USPS. Thousands of orders, mainly made online, were waiting to be fulfilled (KSAT, 2017). The Awalli investigation is but a glimpse of the vastness of illicit activity on the world wide web.

Conclusions

The STOP Act was one of the most recent bipartisan government responses to the opioid crisis, with fentanyl, carfentanyl, and other addictive substances, effortlessly passing our borders via the USPS. Implementing mandatory AED intelligence is only helpful if the data is authentic. Data quality could be an issue for FPO's. However, Executive Director of CBP's Cargo and Conveyance Secure Thomas Overracker stated a regulation package for AED requirements FPO's must follow. This requirements package is due for publication soon. Although the STOP act addressed the significant issue of AED, there are several other issues USPS's Office of Inspector General (OIG) found problematic, and it starts early in the mail distribution chain, including foreign posts. (Overacker, 2020).

Coordinating with foreign posts and inspections and delayed parcels to the ISC's from the inbound foreign commercial flights raises concerns. Per the UPU, the mail should be

submitted to the ISC within two hours after the airplane's arrival; however, the OIG found significant delays, even up to 24 hours (OIG, 2017). A portion of this problem is regarding the ground handlers, which the USPS does not have the authority to manage. Besides this issue, the Postal Service acknowledges the *ramp report*, which monitors the movement of parcels, and its delays need to be done across all the ISC's, not merely a few.

The STOP Act is critical because the intelligence gained on the parcel label of origin can significantly increase the chances of identifying facilitators and networks. Nonetheless, obtaining this intelligence all depends on the capabilities and willingness of postal employees and nation-states abroad, and this requires reliance on foreign posts. The USPS and all entities utilizing our postal system must adhere to this requirement immediately. If analysts and investigators are missing half of the parcel label information, the lack of this essential information makes an investigation that much more difficult.

Information sharing and cross-border cooperation are a must. Criminal organizations possess a level of connectedness that, frankly, law enforcement and intelligence agency do not. Threat networks also achieve an alarming rate of success due to their dexterity and cleverness, willingness to assist each other, the availability of various encrypted communication and payment options.

External to USPS, corrupt entities and bad actors pose a significant challenge to law enforcement operations, evidenced by their ability to participate in illicit trade with near impunity. Internal drug trafficking arrests of postal workers indicate corruption, and the presence of insider threat actors is problematic. Officials in New York arrested five men for running a narcotic trafficking operation, particularly heroin and fentanyl, utilizing the USPS. One of the five men, Daniel Ortiz, was a mail carrier for the USPS who helped facilitate the

shipment of drugs and drug proceeds across the country (United States District Attorney's Office Southern District of New York, 2021). In the wake of their arrest, officials seized over 6 kilograms of fentanyl and heroin that could have permeated into the community, undoubtedly leading to fatal overdoses. In another case, officials arrested 16 postal workers and clerks for knowingly distributing parcels containing cocaine to target addresses in the Atlanta area. The postal workers accepted bribes and recruited fellow employees to partake in the network (Stanley-Becker, 2018).

Having a co-conspirator within the USPS or private mail business, an insider threat renders the goal of supplying the demand of illegal goods that much easier. Like most businesses, employees sometimes fall prey to bribes and end up conspiring with subjects at some point in the supply chain. It is not only falling prey to bribes, as employees making minimum wage are, at times, desperate for money. However, this cooperation with criminal groups is, on occasion, entirely voluntary, or even initiated, and headed by an insider threat. Where supply intersects with the United States Postal system, a mail courier knowingly delivers items that can threaten the health of our communities is a real problem. Interestingly, the Office of Inspector General's 2018 audit report regarding the issue of insider threat was redacted in its entirety (USPS, 2018).

Recommendations

Given the volume of mail worldwide with a destination to the United States, analysts must incorporate advanced techniques into the investigative process of identifying parcels that may contain illicit goods. The Office of Inspector General of the United States Postal Service, in their 2018 audit, proposed enhancements to the USPS's current data model to improve their targeting of suspicious parcels. The data model cultivated information from historical drug

seizures to identify suspicious packages using postal retail, delivery, mail processing, and human resources data (United States Postal Service, 2018). The Postal Service also must improve its inbound mail monitoring and reporting processes by including the actual flight arrival date and time the mail arrives at the airport, improving the paper trail and movement of parcels. The ISC indicated the mail is left susceptible to unauthorized package manipulation (OIG, 2017).

Developing a target parcel can be done close to real-time, as the postal inspector receives a daily list of targeted parcels. One of the main flaws in this data model was the lack of feedback regarding whether a targeted package contained illegal substances, which is a critical source of information. Communication is vital, and USPS recommends an infrastructure that provides near-instantaneous communications between the field and analysts. By incorporating this feedback, analysts and investigators can learn from those key indicators (United States Postal Service, 2018).

Developing a target parcel once inside our borders can be helpful to investigators. Once inside the jurisdiction of the United States, analysts can research the sender and recipient information, IP information, and other techniques used to develop a target parcel to intercept. However, the OECD recommends focusing on stopping illicit trade at the source. The STOP act reflects the need for advanced, secure, electric data before the parcels are loaded onto the aircraft in foreign nations (OECD, 2018).

To tackle the issue regarding corrupt postal workers conspiring with external bad actors, it is recommended to place focus on this interesting intersection where the illicit supply chain and its participants meet with compromised employees of the USPS needs special attention. It should provide a deterrence through swift prosecution. It is also recommended there be a way to

anonymously report suspicious behavior of co-workers as retaliation is real concern to remain quiet.

Dark Web cryptomarkets are selling illicit goods such as firearms with near impunity, as they can circumvent federal firearms laws. A small group consisting of four men in Atlanta, GA, used the USPS to ship firearms, hidden in electronic equipment, to their customers worldwide. Eleven countries assisted the USPS in this investigation by conducting postal audits within their jurisdictions. This intelligence-led investigation helped identify this small criminal network. This investigation provides a perfect example of how cross-border information sharing is necessary and inevitable given the nature of global illicit trade.

The Atlanta investigation also demonstrates the need to dramatically increase websites and social media monitoring. Once shut down, these groups tend to show up again but under a different name. Government and private entities need to form large targeting units to identify these sites, but they can't stop at merely shutting down the websites. Law enforcement needs to follow up by locating and arresting these criminal groups responsible for these sites. Constant public shaming is necessary for social media platforms that have not done their due diligence to identify and immediately shut down these sites and identify the groups behind them.

References

Barksdale, G.R. (2019). Statement of Gary R. Barksdale Chief Postal Inspector United States Postal Service Before the Committee on Energy and Commerce Subcommittee on Oversight and Investigations United States House of Representatives. https://about.usps.com/news/testimony/2019/pr19_cpi0716.htm

Combating the Opioid Crisis: Oversight of the Implementation of the STOP Act: Hearing before the Permanent Subcommittee on Investigations (2020). https://www.hsgac.senate.gov/subcommittees/investigations/hearings/combatting-the-opioid-crisis-oversight-of-the-implementation-of-the-stop-act

Drewewski, R., Sepielak, J., and Filipkowski, W. (2015). The application of social network analysis algorithms in a system supporting money laundering detection. https://www.sciencedirect.com/science/article/pii/S0020025514009979

EPA. (2021). Mail Irradiation. *United States Environmental Protection Agency*. https://www.epa.gov/radtown/mail-irradiation

Federal Register. (2021). Mail Screening Regulations. In *The Federal Register / FIND* (Vol. 86, Issue 98, p. 27823). *Federal Information & News Dispatch, LLC.* https://www.federalregister.gov/documents/2021/09/27/2021-20574/mail-screening-regulations

HSGAC. (2021). Portman, Klobuchar Express Concern Regarding STOP Act Waivers, Urge Biden Administration to Aggressively Pursue Advancing Global Requirements. U.S. Senate Committee on Homeland Security & Governmental Affairs.

Joint Chiefs of Staff (2016). Countering Threat Networks. Joint Publication 3-25 https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_25.pdf

Kimani, Lanzarotta, A., & Batson, J. S. (2021). Rapid determination of eight benzodiazepines in suspected counterfeit pharmaceuticals using surface-enhanced Raman scattering with handheld Raman spectrometers. *Journal of Forensic Sciences*, *66*(6), 2167–2179. https://doi.org/10.1111/1556-4029.14797

KSAT. (2017). Federal investigators shut down drug ring in San Antonio. KSAT News. https://www.ksat.com/news/2017/09/07/federal-investigators-shut-down-drug-ring-in-san-antonio/

Marchand, R. & Kosar, K.R. (2021). The Uncertain Future of the Universal Postal Union. *American Enterprise Institute (AEI).* https://www.aei.org/wp-content/uploads/2021/08/The-Uncertain-Future-of-the-Universal-Postal-Union.pdf?x91208

Narishkin, A. & Cameron, S. (2021). How JFK Customs Searches 1 million packages a day for illegal items. *Business Insider*. *https://www.businessinsider.com/jfk-customs-searches-million-mail-packages-drugs-counterfeit-2019-9*

OIG. (2017). Delayed Inbound International Mail. *Office of Inspector General United States Postal Service. Audit Report Number MS-AR-17-009.* https://www.uspsoig.gov/sites/default/files/document-library-files/2017/MS-AR-17-009.pdf

O'Neill, P. (2021) How police use AI to hunt drug deales on Instagram. Daily Dot. https://www.dailydot.com/irl/instagram-drug-dealing-attorney-general/

Overacker, T. (2020). Combating the opiod crisis: Oversight of implementation of the STOP act. U.S. Senate Committee on Homeland Security and Governmental Affairs Permanent Subcommittee on Investigations. https://www.hsgac.senate.gov/imo/media/doc/Overacker%20Testimony.pdf

Petrossian, G.A., Pires, S.F., and van Uhm, D.P. (2016). An Overview of Seized Illegal Wildlife Entering the United States. *Global Crime*. https://www.crimrxiv.com/pub/u00ggcyo/release/1

Porter, R. (2020). At Permanent Subcommittee on Investigations Hearing, Portman Highlights Need for USPS & CBP to Fully Implement Bipartisan STOP Act. *Rob Portman United States Senator for Ohio*. https://www.portman.senate.gov/newsroom/press-releases/permanent-subcommittee-investigations-hearing-portman-highlights-need-usps

Postal Times. (2021). RedWave Technology Awarded $14M Purchase by the U.S. Postal Inspection Service to Help Protect the Nation's Mail. *The Postal Times.* https://www.postaltimes.com/postalnews/redwave-technology-awarded-14m-purchase-by-the-u-s-postal-inspection-service-to-help-protect-the-nations-mail/

Standaert, M. (2020). Illegal wildlife trade goes online as china shuts down markets. *AlJazeera.* https://www.aljazeera.com/economy/2020/3/24/illegal-wildlife-trade-goes-online-as-china-shuts-down-markets

Stanley-Becker, I. (2018). Postal Service clarifies mission is "mail, not drugs" after 16 workers sent to prison for delivering cocaine. *The Washington Post*. https://www.washingtonpost.com/nation/2018/11/29/postal-service-clarifies-mission-is-mail-not-drugs-after-workers-sent-prison-delivering-cocaine/

TRAFFIC. (2020). Malaysian Stakeholders Discuss Ways to Curb Wildlife Trafficking Through the Mail. *TRAFFIC*. https://www.traffic.org/news/malaysian-stakeholders-discuss-ways-to-curb-wildlife-trafficking-through-mail/

USCBP. (2020). CBP Officers Seize Fake COVID-19 Test Kits at LAX. United States Customs and Border Protection. https://www.cbp.gov/newsroom/national-media-release/cbp-officers-seize-fake-covid-19-test-kits-lax

United States District Attorney's Office Southern District of New York. (2021). U.S. Postal Worker and Four Others Arrested for Shipping Heroin and Fentanyl Through the Mail. (DOJ 21-049). *Department of Justice*. https://www.justice.gov/usao-sdny/pr/us-postal-worker-and-four-others-arrested-shipping-heroin-and-fentanyl-through-mail

United States Postal Service. (2018). Use of Postal Service Network to Facilitate Illicit Drug Distribution. (OIG sAT-AR-18-002) *Office of Inspector General.* https://www.oversight.gov/sites/default/files/oig-reports/SAT-AR-18-002.pdf

USPS. (2019). Guide to Mail Center Security. *United States Postal Inspection Service,* Publication 166. https://about.usps.com/publications/pub166.pdf

USPS. (2014). Publication 14 – Prohibitions and Restrictions on Mailing Plants, Animals, and Related Matter. *United States Postal Service*. https://about.usps.com/publications/pub14/welcome.htm

USPS. (2020). United States Postal Inspection Service Annual Report 2019. *United States Postal Service*. https://www.uspis.gov/wp-content/uploads/2020/02/2019AR.pdf

USPSOIG. (2021). U.S. Postal Inspection Service Oversight of Its Use of Cryptocurrency United States Postal Service Office of Inspector General. https://www.uspsoig.gov/sites/default/files/document-library-files/2021/21-067-R21.pdf

USPIS. (2021). How We Do It: Intelligence Informs our Every Move. *United States Postal Inspection Service*. https://www.uspis.gov/about/how-we-do-it

World WISE. (2016). The World Wildlife Seizures Database. *World Wise.* https://www.unodc.org/documents/data-and-analysis/wildlife/WLC16_Chapter_2.pdf