

2021

Annual Mail Threat Report



RAYSECUR™
THE STANDARD IN MAIL SECURITY

RAYSECUR™
THE STANDARD IN MAIL SECURITY

Table of Contents

Forward to Mail Report	3
Executive Summary	4
U.S. Government Data: Historical Context	6
2021 Mail Threat Statistics	8
2021 Successful Mail-borne Attacks.	12
2021 International Mail Threats	15
2021 Changing Trends in Mail Threats.	18
2021 High Profile Mail Attacks.	20
Mail Threat Snapshots.	24
Looking Ahead to 2022	26
2021 Threat Data in More Detail.	28
Threat Data Center	30
References	31



2021 Annual **Mail Threat** Report

RaySecur's Chief Security Officer Will Plummer analyzes trends from known mail incidents over the last 12 months.

The United States Postal Inspection Service (USPIS) Dangerous Mail Investigations (DMI) Unit responds to 10 dangerous mail incidents every day, on average. Most are undisclosed by law enforcement. ¹

In 2021, several hundred mail-borne threat incidents became public knowledge.

This report presents an analysis of the publicly-known dangerous mail incidents in 2021, within the broader context of official USPIS and Bureau of Alcohol, Tobacco and Firearms (ATF) historical statistics.

Forward

The ability to mitigate and manage risks is a critical success factor in any organization's security strategy. In today's business environment, executives are faced with a rapidly increasing number and types of security vulnerabilities.

Given this evolving risk landscape, many vulnerabilities fall short of the threshold that drives action to address them when viewed in isolation. Executives lack access to the timely, actionable intelligence required to help them understand the probability and impact of potential threats. This lack of information limits an organization's ability to pro-actively implement measures to mitigate them.

Not unlike the current COVID-19 pandemic, many of these events are a low probability, but high impact should they occur. Threats from the mail, including letters and packages, along with physical deliveries to an organization's facilities, are no exception. Over the past 18 months, hoaxes and legitimate dangerous mail attacks have affected Global 2000 corporations and government organizations alike. Viewed in isolation, dangerous mail incidents such as the white powder letters that evacuated Subway's Corporate headquarters or evaded government security to impact Dr. Anthony Fauci, may seem one-off, random events.

The objective of this report is to compile all of the dangerous mail data on an annual basis, providing security leaders with a comprehensive summary of the frequency and very real impacts of these threats, whether legitimate or hoaxes, to inform practical decision making.

Due to the lack of reporting to authorities and differences in how various agencies track dangerous or suspect mail-related incidents, security leaders often struggle to obtain a clear understanding of the magnitude of the problem. As a result, mail threats often lack the attention they deserve. Compared to other threats, such as cyber-attacks or theft, executives often believe the cost and impact of a mail incident can be absorbed. Yet, recent events have forced organizations to reassess their risk management matrix as it applies to mail.

The direct costs to affected organizations are very real and can quickly run into the millions of dollars, even for hoaxes resulting in a temporary shut-down of a data center, production line, or corporate campus. Recovery costs for viable threats are often significantly higher, one notable example being the remediation costs

for impacted U S government facilities following the 2001 anthrax letter events which ran into the hundreds of millions. Beyond the direct costs, indirect costs can be significant but difficult to quantify, such as reputational damage to the brand, negative publicity, intangible impacts to employees, and customer perception. This report highlights current trends in mail threats, their prevalence, and impacts to better support the enterprise risk management process and enable security practitioners to make informed decisions.

RaySecur annually catalogs all mail-borne threats reported to the media to capture the growing incidence of mail threats across the globe. For the first time, this year's annual mail threat report also includes international events, to aid global organizations in accurately assessing their risk across all regions in which they operate.

As in year's past, we aggregate individual events with official government statistics from organizations including the USPS, ATF, and the Federal Bureau of Investigation (FBI) to generate the intelligence in this report.

Readers should be aware that considerations have been made as each government agency views and categorizes threats differently. For example, the definition of a "suspect package" has a different meaning when categorized by the USPS, ATF, and the FBI.

In addition to presenting summary statistics, individual cases are highlighted to provide further details relevant to the security practitioner. I hope you find this report informative, and more importantly, that the information provided here helps inform and mitigate mail-related risks to you and your organization.

Sincerely,



Will Plummer
Chief Security Officer



Prior to joining RaySecur as Chief Security Officer, Will spent 25 years in the US Army.

AWARDS AND DECORATIONS

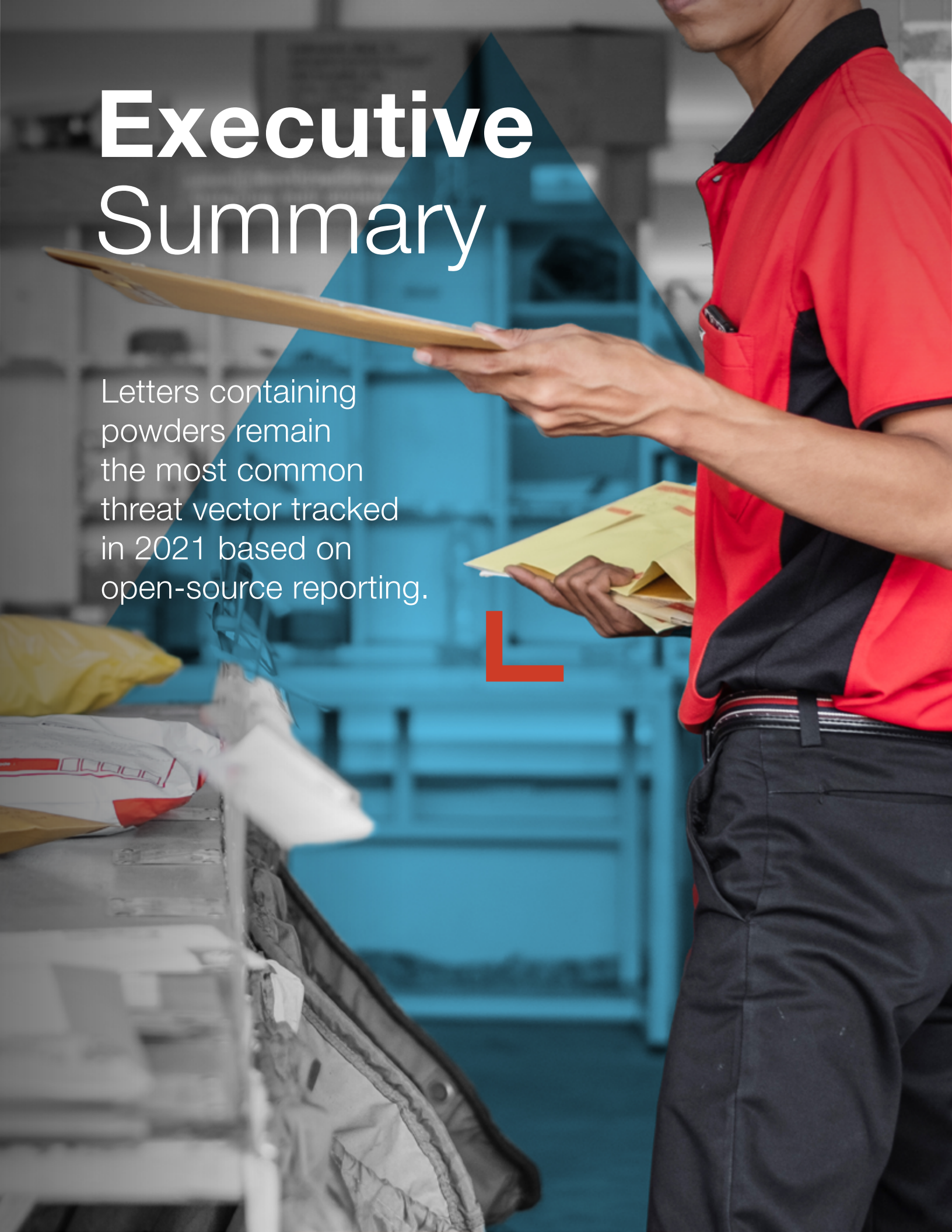
- Presidential Unit Citation
- Meritorious Unit Citation
- Bronze Star with "V" and Oak Leaf
- Meritorious Service Medal with 4 Oak Leaf
- Combat Action Badge

TRAINING AND CERTIFICATIONS

- Naval School Explosive Ordnance Disposal
- FBI Hazardous Devices School
- Advanced Access and Disablement
- Chemical Energetics Course
- ATF Post Blast
- FBI Post Blast
- Foreign Weapons Intelligence Course
- Global Antiterrorism Operator Readiness Course (Director)
- Bomb Technician Robotics Course
- Demonstrated Senior Logician
- HAZWOPER
- TSCM
- Anti-Terrorism Force Protection Certified
- Army Instructor Training Course
- Systems Approach to Training
- Equal Opportunity Leaders
- Hazardous Material Waste Handling

Executive Summary

Letters containing powders remain the most common threat vector tracked in 2021 based on open-source reporting.



These figures come from the most recently published data reported by the ATF and USPIS.



262K

Suspicious mail items analyzed



6.3K

Mail incidents reported

The *Threat Data Center (TDC)* is an informational product prepared by RaySecur utilizing open-source reporting to present a comprehensive view of the state of mail-borne threats. While official government data sources provide a historical view of both the prevalence and magnitude of dangerous mail threats, the publication of official statistics typically lags actual incidents by six to twelve months. The objective of this report is to summarize key statistics from official data sources to frame the problem, while also providing accurate and timely information on current threats.

The most recent 2020 reports on suspicious mail and packages by the ATF and the USPIS detailed over 6,300 incidents in the United States that elicited a response from either agency.¹ These numbers represent a 28% decline from the prior year and are most likely attributable to the effects of the pandemic. While official incident reports fell in 2020, the overall impact on targets remained high, with 42 injuries reported based on open-source data, 63% of which were delivered in the form of letters and all attributed to powders.

The effects of COVID lockdowns, vaccination mandates, and other societal stressors continue to reshape the threat environment on a daily basis. The public-domain 2021 data as identified in the TDC reflects an upward trend, although official numbers have yet to be released. Several of these incidents required significant responses

and, as a result, are changing how organizations manage future threats.

The first reported threats of 2021 occurred after the January sixth attack on the U.S. Capitol, where courts, judges, and lawyers received threats in response to the federal charges filed against the participants. The continued controversies related to COVID-19 vaccines saw laboratories and vaccination facilities worldwide receive suspicious packages and white powder threats intended to shut down production. Globally, successful threats included explosive mail incidents in Germany resulting in several injuries, as well as white powder threats sent to multiple targets in Hong Kong.

Target locations for mail threats spanned businesses and government offices to private residences, as witnessed by threats sent to U.S. government leaders, including Senator Rand Paul's home, Congresswoman Ilhan Omar's headquarters, and Director of the National Institute of Health Dr. Anthony Fauci's office, despite prior security screening.

Based on the aggregate data compiled from the public-domain sources in 2021, 89% of dangerous mail attacks involved letters or parcels small enough to fit in a curbside drop box – highlighting the vulnerabilities posed by small items with an unknown chain of custody. Of these threats, white powders, including drugs, were the most prevalent, being found in 54% of dangerous mail items.

Beyond the statistics, the dangerous mail incidents covered in this report span everything from entire organization shutdowns to home evacuations. Whether it is a hoax or real, these threats force losses in revenue, time, and the sense of security, and highlight the often-unnecessary exposure to risks.

Legitimate mail attacks sent innocent bystanders and first responders to hospitals for exposure to threats such as fentanyl, ricin, and explosive devices. Despite the prevalence of these incidents, their impacts can be mitigated by raising awareness and implementing relatively straightforward measures once the risks are understood.



WHITE POWDER THREATS ON THE RISE

Substances ranging from deadly to benign, all capable of triggering a response.

- Anthrax
- Ricin
- Flour
- Sugar
- Baking Powder

U.S. Government Data: Historical Context

The primary sources of official data on dangerous mail attacks and hoaxes are the USPS and the United States Bomb Data Center (USBDC) managed by the ATF.

U.S. POSTAL
INSPECTOR
POLICE





1.3K

USPIS Inspectors, 400 in DMI focusing exclusively on mail threats



10

Average daily mail threats USPIS and ATF responded to over the last three years
(aggregate data from USPIS and ATF annual reports 2020-2018)

The USPIS and ATF catalog incidents differently, and the methodology for reporting even within the same agency may vary from year-to-year. Complicating matters further, many of these events do not make it into the news cycle.

Nonetheless, these sources serve as an indicator for the prevalence of mail threats and the magnitude of their impacts across the United States.

The USPIS Dangerous Mail Investigation (DMI) unit consists of over 400 federal agents responsible for responding to incidents that involve the mailing of suspicious and hazardous substances, including chemical, biological, radiological, and explosive items (CBRNE).²

Although official 2021 numbers have yet to be released from the USPIS, over 262,000 suspicious mail items were sent for forensics analysis in the previous year, with inspectors responding to over 2,356 incidents involving suspicious items,

powders, or liquids sent in the mail. In addition, dangerous mail events related to suspicious substances and restricted matter, including CBRNE weapons, hazardous items, and hoax threats, resulted in 184 new cases, 95 arrests, and 79 convictions, in 2020 brought by USPIS alone.³

Similarly, the USBDC reported 3,950 suspicious or unattended package incidents in 2020. Of these, approximately 934 incidents involved letters or parcels and another 775 incidents were not categorized. In addition, 984 explosion incidents, of which 428 were classified as bombings, occurred in 2020, resulting in 91 injuries and 13 fatalities.⁴

MOST INCIDENTS INTEND TO CAUSE WORKPLACE DISRUPTIONS

Letter or package bombs usually target specific individuals. Placed threats however, are generally intended to disrupt workplaces and injure indiscriminately. Bomb threats may target either individuals or organizations. Revenge is the motivation that most often triggers each of the three types.⁵

In order to provide key stakeholders with timely information, given the fragmented and delayed nature of official reporting, RaySecur actively tracks events in the public-domain, providing up-to-date information in our Threat Data Center. This information is sourced from local, state, and national media outlets, as well as public records. The remainder of this report highlights key incidents and trends based on this data from 2021.



2021 Mail Threat Statistics

The following statistics are compiled from the 250+ dangerous mail incidents that occurred in the United States and were reported in the media in 2021.



These events represent a small fraction of the total, many of which are handled internally, or are reported to law enforcement but do not make it into the public domain.

Not only was there a rise in dangerous mail incidents, but also the TDC highlights changes in threat trends. In 2021, letters containing written threats rose 34%.

In addition, 2021 saw 20 dangerous mail related injuries, the majority were due to powders or drugs including fentanyl, suboxone, and unidentified powders.

The prevalence of powder threats and drugs, including fentanyl which is deadly even in small quantities, is alarming as most mail screening in government and private sectors is conducted using X-ray scanners.

Due to the low mass of powder in the letter, these threats can evade conventional X-ray screening methods.

The PAS 97 2015 specification by the Centre for the Protection of National Infrastructure (CPNI) is the standard for mail security screening in the United Kingdom.⁶

The specification contains several comments on the challenges of conventional X-ray approaches in screening for powder threats.

About the Data

Most law enforcement agencies do not publish their logs in a manner conducive to aggregate analysis and the data is often delayed. Therefore, RaySecur tracks mail-specific threats using open-source data, compiled from national, state, and local media sources, updated regularly.

Accurate, timely, and actionable intelligence is critical to plan and prevent dangerous mail attacks.

This report is intended to provide a snapshot of recent mail threats and dangerous mail attacks to enable security professionals to plan and implement mitigation measures accordingly. These data are analyzed along with events reported by the USPIS and ATF. The ATF operates the USBDC, the clearinghouse of record for information on incidents involving arson and the suspected criminal misuse of explosives. The USBDC collects data from U.S. law enforcement, military and public safety agencies, and produces its annual Explosive Incident Report (EIR).

The ATF and EIR are extremely useful for trend analysis, however their data are generally tied to criminal activities and prosecution. Many incidents fail to meet the ATF's reporting requirements, and are therefore omitted from their data and left unreported. RaySecur's dataset also includes dangerous mail incidents which may not meet ATF reporting requirements.

CPNI

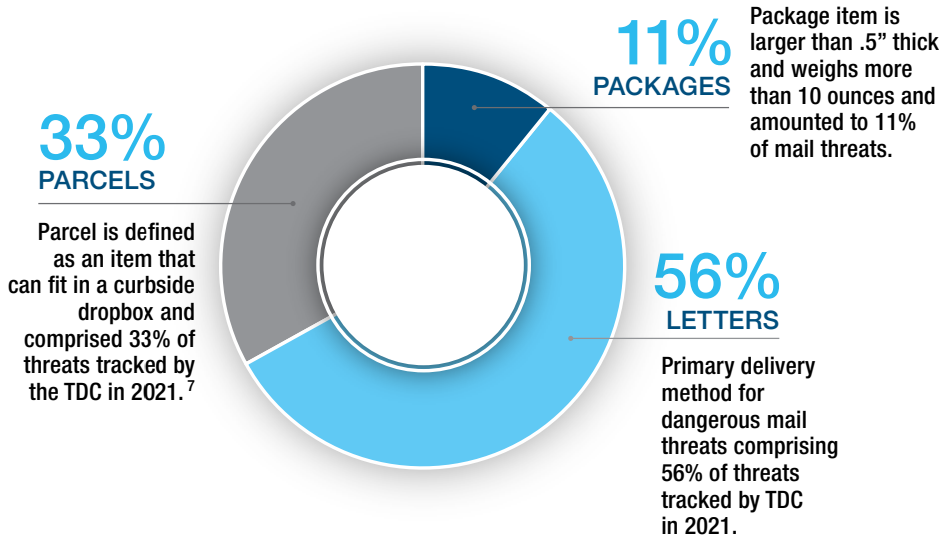
Centre for the Protection
of National Infrastructure

“ Such materials may not be “white” and may not be “powders”; materials may be crystalline (e.g., sugar), oily or waxy residues, or liquids, and might be present in sufficiently small quantities as to be undetectable by typical X-ray-based screening processes.” – PAS 97 2015

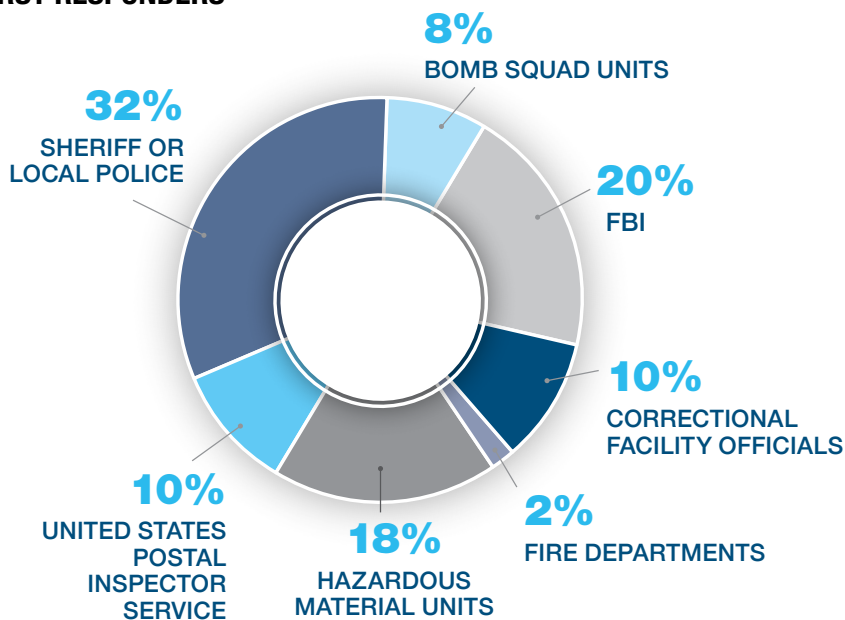
EFFECTIVENESS

59%
CAUSED A RESPONSE
 Mail stream attacks were successful in either causing harm or disruption to the recipient.


DELIVERY METHOD



FIRST RESPONDERS



GEOGRAPHY

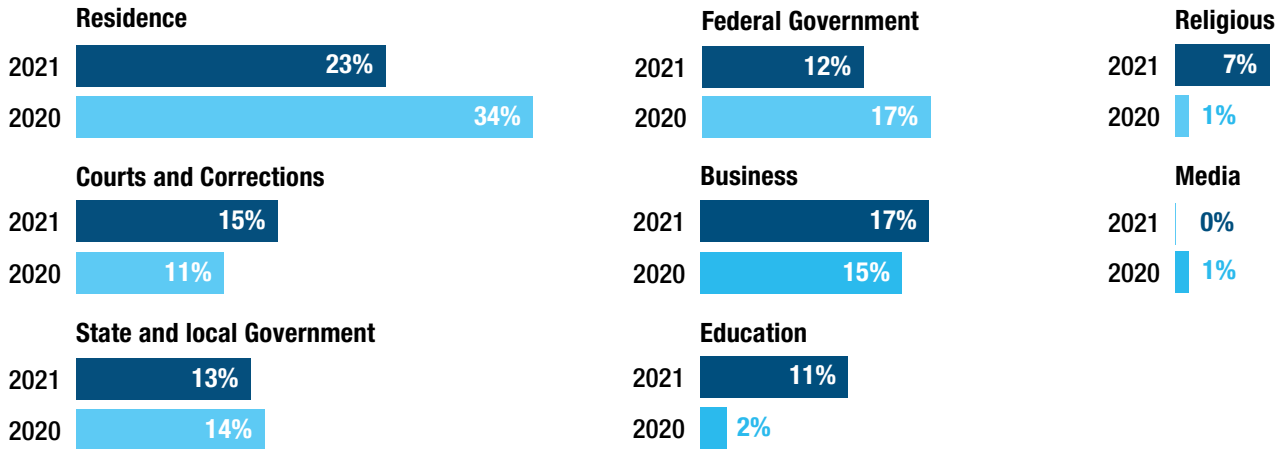
 **TOP 5 US STATES**

1	New York	10%
2	Texas	9%
3	Pennsylvania	7%
4	Georgia	7%
5	Alabama	7%

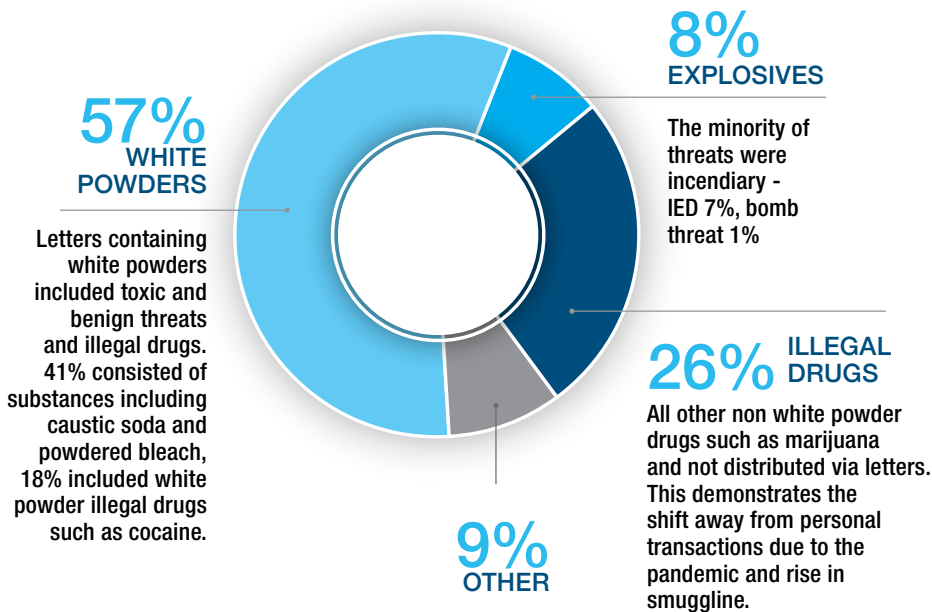
 **INTERNATIONAL COUNTRIES**

1	Europe	35%
2	Asia	30%
3	Oceania	17%
4	Canada/Mexico	14%
5	Africa	3%

TARGETS



SUBSTANCES



TOP 10 SUSPECTED SUBSTANCES*

1	Ricin	19%
2	Anthrax	18%
3	Other Drugs	18%
4	Marijuana/THC	11%
5	Unknown	7%
6	Cocaine	6%
7	Fentanyl	5%
8	Methamphetamine	5%
9	Other	5%
10	Suboxone	3%

* As suspected by first responders prior to lab testing.



┌

2021

Successful Mail-borne Attacks



59%

**OF MAIL THREATS
TRIGGERED A
RESPONSE**



20

**INJURIES
REPORTED IN U.S.**



COVID-19

**MANDATES
SOURCE
OF UNREST**

The number of mail threats, based on public media reports, increased in 2021 over the previous year due to a myriad of reasons and included several recurring themes. Occurring throughout the year were events based on mistrust or anger against the U.S. government resulting in threat incidents at local, state, and federal facilities - originating from both sides of political views. Individuals impacted by COVID-19 restrictions or vaccine mandates caused significant friction and negative responses.

One recurring theme from 2021 was backlash, often from employees (insiders) or customers due to corporate COVID vaccine mandates and masking policies. A number of prominent corporations implemented vaccination requirements for their staff and imposed penalties or terminated employees who did not comply. In some cases, employees working remotely were terminated for refusing to be vaccinated and were then required to return company equipment via the mail, opening the floodgates to parcel threats from disgruntled employees.⁸

Threats involving the mail fall on a broad spectrum from no identified threat to a legitimate CBRNE risk. A benign powder is more than adequate if the intention is to disrupt daily life and not maim or kill. For example, a successful mail

threat doesn't require the risk or sophistication required to send ricin toxin when a small quantity of bread flour has the same result. Of the 20 injuries reported in 2021, the number one threat was fentanyl and the second was chemicals.

In 2021, nearly 59% of all mail threats were viable, meaning that overall, whether the mail contents were drugs or a powder threat, the item triggered a legitimate response and some disruption to daily operations at the intended recipient or along its distribution route. When threats were not viable, they often were strange items, odd packaging, or suspicious labeling that caught the screener's attention and elicited some type of response, but were

deemed benign (false alarm) and constituted neither a hoax nor a legitimate threat.

All the incidents and statistics highlighted in this report were sent through the mail stream and delivered to the target recipient, or were last-mile threats where the threat was dropped off under the guise of regular mail.

International dangerous mail events are at a greater risk of last-mile threats due to the higher amount of courier services and less scrutiny on the method of delivery.



Last-mile threats, where the package is carried to the target and left as a standard delivery, bypass a chain of custody and represent a legitimate risk to organizations and facilities

Predominant Targets of Interest

Political leaders and government facilities were **targeted 15% more often in 2021, rising to 49% from 42% in 2020**. These targets were generally high profile, received white powder and threatening notes, and drew a response from federal authorities.

Federal courthouses, judges, and lawyers were **hit with primarily white powder threats** in response to the January sixth prosecutions throughout the first half of the year. One of the largest groups that saw a significant increase was state and local government leadership, usually responding to masking mandates.

Religious locations and leaders saw **an alarming increase from 1% to 7%**. This rise is directly tied to a rash of racist letters sent to churches across the south. Racially motivated mail threats also increased dramatically across all minority groups.

The number of **threats against corporations stayed consistent at 15%** of mailed threats even though most offices were operating with minimal staffing. With the return to work and vaccination mandates in place, the latter half of 2021 was more active.

Most business-related events occurred at **satellite facilities**, away from the main offices, and included a spate of racially motivated hate threats to small companies that supported societal changes. When a larger office or corporate headquarters was targeted, most of the incidents were threats from insiders regarding company policy.

The **distribution of illegal drugs** remained consistent with last year's numbers, with only a **slight increase from 17% to 19%**. There is a noted increase in the amount of illicit drugs getting into prisons and jails through the mail disguised as legal mail where the prisoner has an assumed right to its

delivery. While the overall increase was small for the category as a whole, the **increase over 2020 is partially attributed to homemade counterfeit pills** meant to mask the actual ingredients, usually fentanyl.

The past year also saw a shift with increasing numbers of mail items containing drugs sent to businesses. As such, organizations have been forced to adopt policies on handling illicit and illegal items within their mailrooms.

Residences were targeted less frequently in 2021, dropping from 34% of dangerous mail targets in 2020 to 23% in 2021. This shift is partly attributed to people gradually returning to the office and to threats shifting to focus on government targets. Many residential events remain drug-related as the pandemic pushed a significant amount of illegal substance transactions to the mail stream.



2021 International Mail Threats

The risk of a mail threat incident, when compared to the U.S., is:⁹

3X
higher in
Western Europe

10X
greater in
Southeast Asia

20-40X
greater in Africa and
the Middle East,
respectively

2X
higher in
South America

Mail incidents have a higher chance of occurring abroad

International Threats on a Similar Trajectory as Domestic Attacks

Unlike the data for the United States where official source data is regularly cataloged by various government agencies including USPS, ATF, and FBI, international data is much more fragmented. Many countries do not publicly report mail threat statistics, which makes understanding specific mail risks in a particular region all the more challenging.

One proxy for gauging the potential for mail threats in a particular part of the world is the global terrorism risk index, as mail threats and dangerous mail events are generally categorized as terrorist events. The Global Terrorism Database (GTD), managed by the National Consortium for the Study of Terrorism and Responses to Terrorism (START) catalogs more than 200,000 terrorist attacks globally.

The motives behind mail threats on the international front range from social unrest to insider threats targeting corporations. In addition, unstable local or

national government infrastructure, internal political conflict, or other destabilizing factors which vary from country to country also play a role and can be used to estimate the likelihood of an incident.

While mail threats are often thought to be most prevalent in the United States, based on popular media reporting, the reality is that the probability of a terrorist incident, including a dangerous mail event, is often greater abroad. Based on historical data from the GTD over the past decade, the frequency of a terrorist event occurring is nearly three times greater in Western Europe than in the United States.⁹

Based on public-source media reports for 2021, international threats involving mail were significant and targeted corporations, governments, and individuals at all levels. The recipient of the most threats were governments and national-level leadership, with the common reasons being masking, vaccines, and work restrictions related

to COVID. Depending on the country and the severity of the government's response, mail became one of the only methods to projecting threats. The many COVID lockdowns, border closings, and restrictions also led to more drug smuggling attempts via the mail throughout the year.

Other world events also drew negative attention. Hong Kong, for example, saw repeated white powder events aimed at leadership who were thought to be supporting the Chinese efforts on the island. Each time the event reached the international news cycle for both the incident and the response. Similarly, France, Australia, Canada, Germany, Spain, and India received threat letters delivered to high-level leadership even after the screening process was completed. Government leadership will always be targeted, making screening smaller, high-volume mail more critical to security.

Many of the threats aimed at government targets were political and pointed to frustrations or



perceived failures of leadership. The police in Italy disclosed that Pope Francis received a package containing bullets - "The three bullets are presumed to be for a pistol, and the envelope also contained a message alluding to financial operations at the Vatican."¹⁰

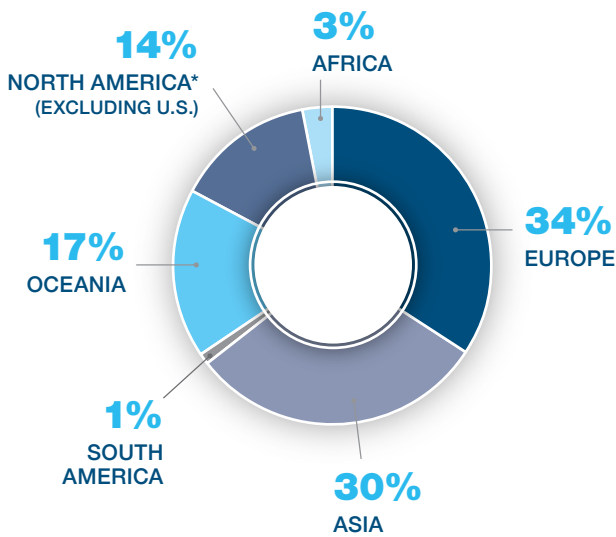
Corporate entities were also heavily targeted. For some individuals, companies have become living entities. With that comes the public acting out to the company as a whole and not the individuals within it. In Germany, several corporations, including Lidl, Hipp and Wild Drinks were hit with three letter bombs.

The first detonated, injuring three and causing a national response to locate the perpetrator. The second caught fire, and the third was stopped at a postal facility en route to the target. An individual initiated the attack with no ties to any of the three companies. When charges were brought, he could only answer that he was "angry."¹¹

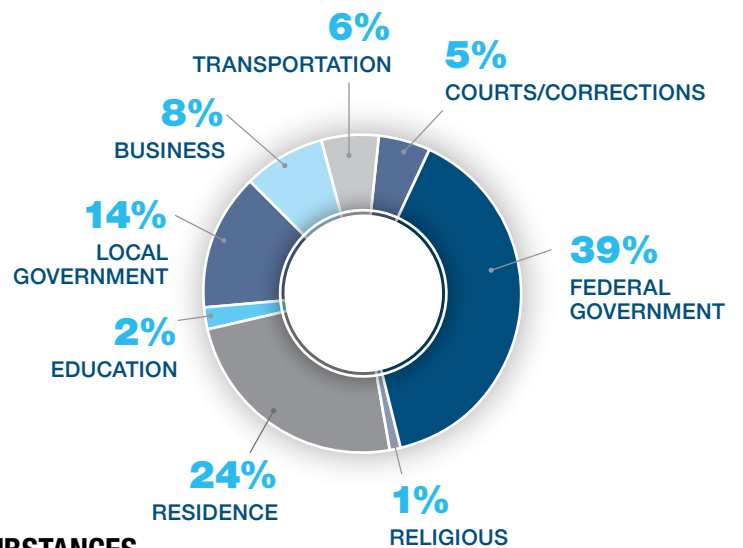
Similar to the events in Germany, reports showed that corporations generally received functioning explosive devices out of anger. For instance, AstraZeneca's vaccine plant received a hoax device intended to stop production in response to the development of covid vaccinations.¹²

It should be noted that while the data presented here provides an indication of the frequency and types of dangerous mail incidents which occurred globally in 2021, the data is aggregated from reports in the public media. As such, it is most likely biased toward legitimate events focused on high-profile targets which garner international media attention. Reporting on these events also varies from country to country. The reader is advised to consider these limitations when interpreting this data.

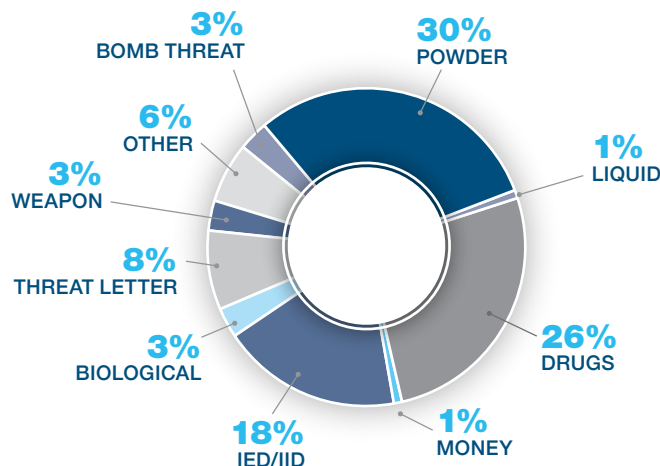
CONTINENTS



INTERNATIONAL TARGETS



INTERNATIONAL SUBSTANCES





2021 Changing Trends in Mail Threats

Emerging Threats

While the incidence of white powder threats remained similar to last year, the actual material increased in toxicity. Instead of the typical benign powders, letters now included dangerous powdered bleach, caustic soda, ricin, and other irritants.

Fentanyl, which can be deadly in quantities as small as 1 mg is also of growing concern, and resulted in the hospitalization of multiple employees from mail-borne threats in 2021.

The inclusion of harmful materials has caused an increased in legal charges filed against the perpetrators, as it shows intent to harm, and with it, more severe penalties.

Hate crimes, death threats, and extorsions rose sharply from 8% to 25% and with it a heightened response by federal authorities.

The continued racial threats against the Asian American community increased this year and are tied to the perception that the pandemic originated in China, with events aimed directly at individuals, churches, and small business owners.

Other high-profile race targets include the DuSable Museum of African American History, which continues to receive hate mail and is used as an outlet for either personal or political beliefs.¹³

These race-related events rose significantly during the summer months. They were tied to the social unrest across the country and increased in volatility the longer each period of protest endured.

Convergence of Mail and Cyber Threats

New cyber and physical threats are increasingly converging to form “cyber-physical threats.” One prominent example is, “warshipping,” where a micro-electronic device is mailed into a facility concealed within a mail item or gift. These types of devices, first reported by IBM in 2019 may form a local network access point, providing an attacker with access to local networks via a cellular connection. Such devices are small enough to be concealed between two sheets of cardboard forming a false bottom or side of a box or small flat-pack shipping envelope.¹⁴

Organizations with backlogged mail due to facilities closures are particularly at risk for these types of threats, as unopened mail items pile up in warehouses and employee’s desks. Implementing a continuous screening process, minimizing the storage of unscreened mail items, and quickly discarding packaging are simple methods to mitigate such threats.

Additional mail and cyber threat vectors include storage devices and USB drives. Once considered benign, USB drives have reemerged as a viable threat, with cybercrime groups mailing out significant quantities. When a recipient uses an infected drive, the installed ransomware is automatically deployed and spreads throughout the network seeking other systems to hijack. With the increase in ransom payments and the entrance of cyber insurance, this trend will likely increase through 2022.



7

2021 High Profile Mail Attacks

Dr. Anthony Fauci's Comments on Receiving a White Powder Letter



Were you ever shot at or confronted?

No, but one day I got a letter in the mail, I opened it up, and a puff of powder came all over my face and my chest. That was very, very disturbing to me and my wife because it was in my office.

So I just looked at it all over me and said, "What do I do?" The security detail was there, and they're very experienced in that. They said, "Don't move, stay in the room." And they got the hazmat people. So they came, they sprayed me down and all that.

Did they test the powder?

Yeah. It was a benign nothing. But it was frightening. My wife and my children were more disturbed than I was. I looked at it somewhat fatalistically. It had to be one of three things: A hoax. Or anthrax, which meant I'd have to go on Cipro for a month. Or if it was ricin, I was dead, so bye-bye.¹⁵

Lidl, Wild and Hipp Receive Letter Bombs

Prosecutors in Germany are investigating a possible link between three recent letter bomb attacks on German food retail companies. "We assume there is a connection," state prosecutors in Heidelberg said on Friday after attacks on a supermarket chain, a drinks company, and a baby food producer this week. They said further attacks were not likely but could not be ruled out entirely.

On Wednesday night, they confirmed that an explosive had been identified and disarmed at a parcel distribution center at Munich airport. The parcel was addressed to the Bavaria-based baby food company Hipp.

Three people were taken to hospital on Wednesday when a letter bomb exploded at the German headquarters of the discount supermarket Lidl. Around 100 people were evacuated from the building in Neckarsulm, western Germany. A similar explosion was reported in nearby Eppelheim at the Wild drinks company, whose products include Capri-Sun.¹⁶



Senator Rand Paul Receives White Powder Threat



A suspicious package containing white powder was sent to the home of Sen. Rand Paul, R-Ky., his office said Monday. Investigators later determined the substance was not hazardous, a law-enforcement source told NBC News.

“I take these threats immensely seriously. As a repeated target of violence, it is reprehensible that Twitter allows C-list celebrities to encourage violence against me and my family,” Paul tweeted.

The suspicious package, which was sent to his Kentucky home, contained a white powder, his office told NBC News. The envelope was examined for harmful substances and investigated by the FBI and Capitol Police.

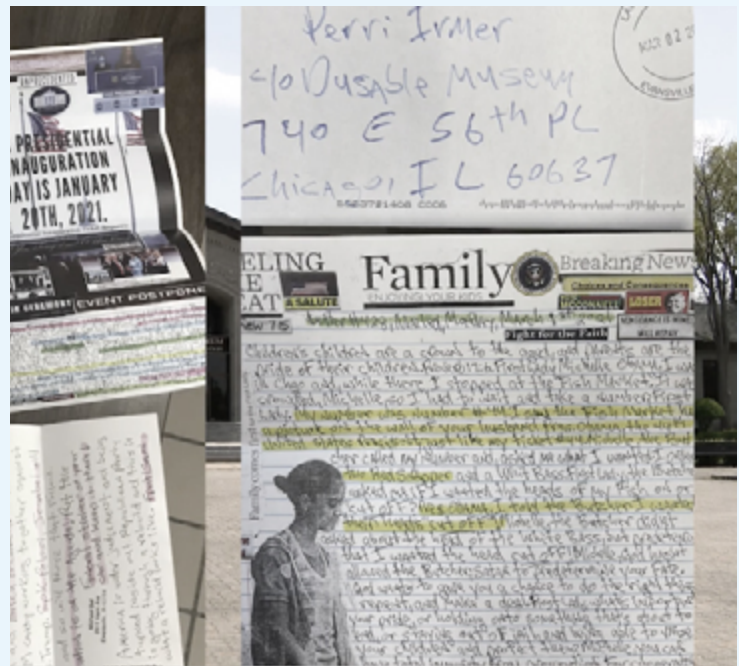
The law enforcement source said initial testing of the substance determined it was not dangerous. In a statement, the Capitol Police said that as a precaution, the substance is being taken to a lab “for further testing.”¹⁷

Minority Museum Receives Threat Letters

The president and CEO of the DuSable Museum of African American History went public Tuesday with news of a series of threatening letters that began after the Capitol insurrection and shortly before the Biden/Harris administration took office.

“They were targeting us as a conduit to other Black leaders, threats against President Biden, Vice President Kamala Harris, even Nancy Pelosi,” said president and CEO Perri Irmer. “The minute I saw the content of this mail, I reached out to the U.S. Secret Service.”

In all, the museum, which is the nation’s oldest independent Black museum, has received six letters espousing hate and vitriol since January 22. The latest one received was last Friday, April 23. The museum has also encountered threatening letters in the past, during former President Barack Obama’s tenure.¹⁸



Hong Kong Courts Receive Dangerous Powder

Letters containing highly corrosive substances were delivered to two Hong Kong courts on Tuesday, prompting the deployment of bomb disposal officers and sparking the second round of evacuations in less than a week related to judicial intimidation.

One letter sent to Sha Tin Court was addressed to Magistrate Pang Leung-ting, while the other, sent to West Kowloon Court, was intended for Deputy Judge Kathie Cheung Kit-ye, who was also the target of a similar delivery last week, according to a police source. The source said Tuesday's letters were found to contain lye, also known as caustic soda or sodium hydroxide, a substance capable of causing chemical burns. It is used in a variety of manufacturing processes.¹⁹



Parcel Bomb Detonates and Injures Four



Four police officials, including a lieutenant colonel, were injured after a parcel bomb went off at the Criminal Investigation Department (CID) headquarters in Naypyitaw, Myanmar on Tuesday evening, according to police sources.

The parcel, which had been labeled as evidence, exploded when police officials opened it, said an official who requested anonymity.

“The parcel was among the evidence packages for explosion cases sent from other towns,” the official told Myanmar Now. One officer, Police Lt-Col Zaw Than, sustained serious injuries to his leg, the source said. Details of the injuries to the other three police officials were unknown at the time of reporting. Another police official in Yangon confirmed the bomb blast at the CID headquarters but refused to disclose further details.²⁰



POLICE

Mail Threat Snapshots

Sampling of events
throughout the year.



Law Firm Used as a Political Target

A threatening letter containing white powder arrived at a high-profile law office, triggering a hazmat response and an FBI investigation. The targeted lawyer was tested and cleared by a doctor, and the powder was determined to be corn starch. The letter with a single line of “You will NOT represent these traitors,” and a line from Shakespeare’s Henry VI, Part 2, “Let’s kill all the lawyers.” was likely triggered by the announcement the firm was representing Jacob A. Chansley, who was in the U.S. Capitol during the riot on January sixth.²¹

Disgruntled Ex Employee Targets Business

An Oregon man pleaded guilty to sending former coworkers letters containing a white powder he said was anthrax. The white powder contained in the letters was not anthrax but a toxic pesticide. The letter simply said “Merry Anthrax” and “Eat (expletive) and die. More to come,” the U.S. Attorney’s Office said.²²

Harmful Substance Sickens Recipient

Police investigated after two people fell ill after opening a suspicious package. Respondents included the police, fire department, and an ambulance crew for a call of two residents experiencing dizziness.²³

White-Powder Threat Against Local Business

The United States Postal Inspection Service, the Houston Police Department, the Houston Fire Department, and two hazmat units assisted the FBI in Houston in reviewing suspicious mail, including two letters, sent to a local jewelry

store. The dozen or so pieces of mail, some containing substances, were sent to the Houston store over a week-and-a-half period from a man in Redding, California. The employee that opened the mail stated, “When I opened it, there were white crystals in the package. I’ve seen anthrax, I knew it wasn’t anthrax, but you never know what it is.”²⁴

Vengeful Act

A registered nurse admitted to police that she sent packages with human feces and a letter containing a bloody sanitary pad to her husband’s ex-wife. The packages and letters were sent through the U.S. postal mail, and allegedly the perpetrator had been stalking and harassing the victim for months.²⁵

Prisoner Sends Mail Threat to Court

A circuit court employee received and opened a letter addressed to “Clerk of Courts” that said, “I am going to bomb every judge in the Washington County Courthouse if I don’t get let out of jail by July fourth.” The letter was sent in the name of an inmate, who was determined not to be the sender, and the writing was sloppy with obvious spelling corrections.²⁶

Prisoner Mail Screening Stops Illegal Drugs

Corrections officers recovered 19 orange strips of Suboxone in an inmate’s mail delivery that were hidden inside the battery compartment of a watch mailed to the prisoner.²⁷

State Lawmakers Vote Spur Threats

Several members of Idaho’s political staff received mail threats over how they voted on laws intended

to reduce wolf numbers in the state. The unsigned letter read, “just as the wolf went from predator to prey, so shall you. It is not your place to play god, but if you will then, so shall I.”²⁸

Bomb Squad Responds to University Campus

The Community Engagement and Student Success building at the University of Texas Rio Grande Valley was forced to evacuate after receiving a suspicious package containing a “fake explosive device.” The bomb squad responded to the incident and ultimately detonated the package. While the package proved to be harmless, the university suspended operations for over two hours to ensure staff and students’ safety.²⁹

Federal Politician Target of Threat

The office of U.S. Rep. Ilhan Omar, D-Minnesota, received a package with a “suspicious substance” and a threat reading, in part, “The Patriarchy will rise again.” The Capitol Police responded, and law enforcement ultimately confirmed that the substance was not hazardous.³⁰


FBI Warns Broadcast Media of Threats

The FBI office in New York placed local television stations on warning to be alert for letters from someone claiming to be the “Chinese Zodiac Killer” after several media outlets in the Albany area received letters. In its statement, the FBI informed the television stations of the potential threats and to not tamper with any they may receive to help preserve possible DNA evidence.³¹



Looking Ahead to 2022

White powder threats continued to rise numerically, but more importantly, the shift from benign to more hazardous materials means that offenders aren't simply focused on a general disruption of the workplace but on also causing actual harm to recipients. The increased mail distribution of illegal drugs, like fentanyl or methamphetamine, and toxins, including caustic soda and powdered bleach, require immediate decontamination and can't wait for a response team to neutralize the threat. Therefore, organizations require higher-level response capabilities to react to employee safety immediately.




The daily upheaval felt by businesses and individuals over the past year has continued in 2022 with the emergence of the Omicron variant and often confusing safety requirements, culminating in an increased risk of mail threats. Consistent with previous years, the actions and policies implemented in 2021 will have ripple effects in the coming months. The world will watch the reaction to government and private companies' mandatory workplace vaccinations, deepening stress on a changing or now absent workforce, and the general increase in the cost of living. The expectation is that retaliatory mail threats will continue in response.

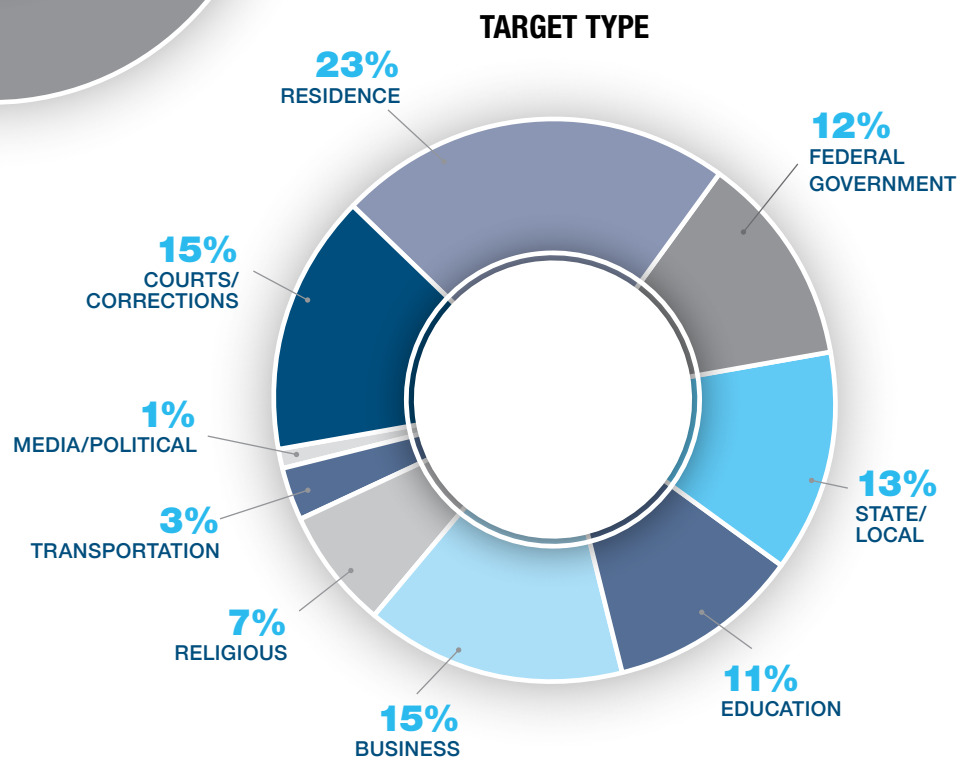
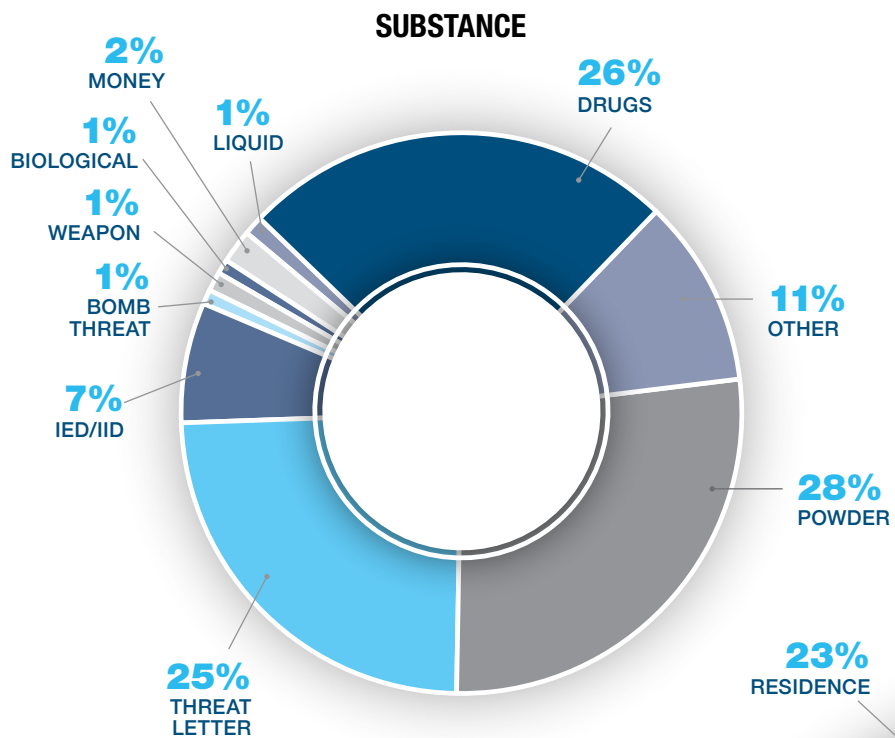
The push for mandatory vaccinations and the subsequent fallout has significantly affected all aspects of daily life. The first vaccine requirements have given way to layoffs, extra testing, and penalties for noncompliance. Companies, mostly with remote workers, who lay off employees for not following established vaccine policies, should anticipate suspicious packages from insider threats, historically the source of most mail threats.

Tainted mail has been used throughout the pandemic to target government facilities, hospitals, vaccination clinics, and other health-related verticals, often escalating to more aggressive events. These targets now face threats they are often unprepared for and with staff unable to adopt a defensive posture.

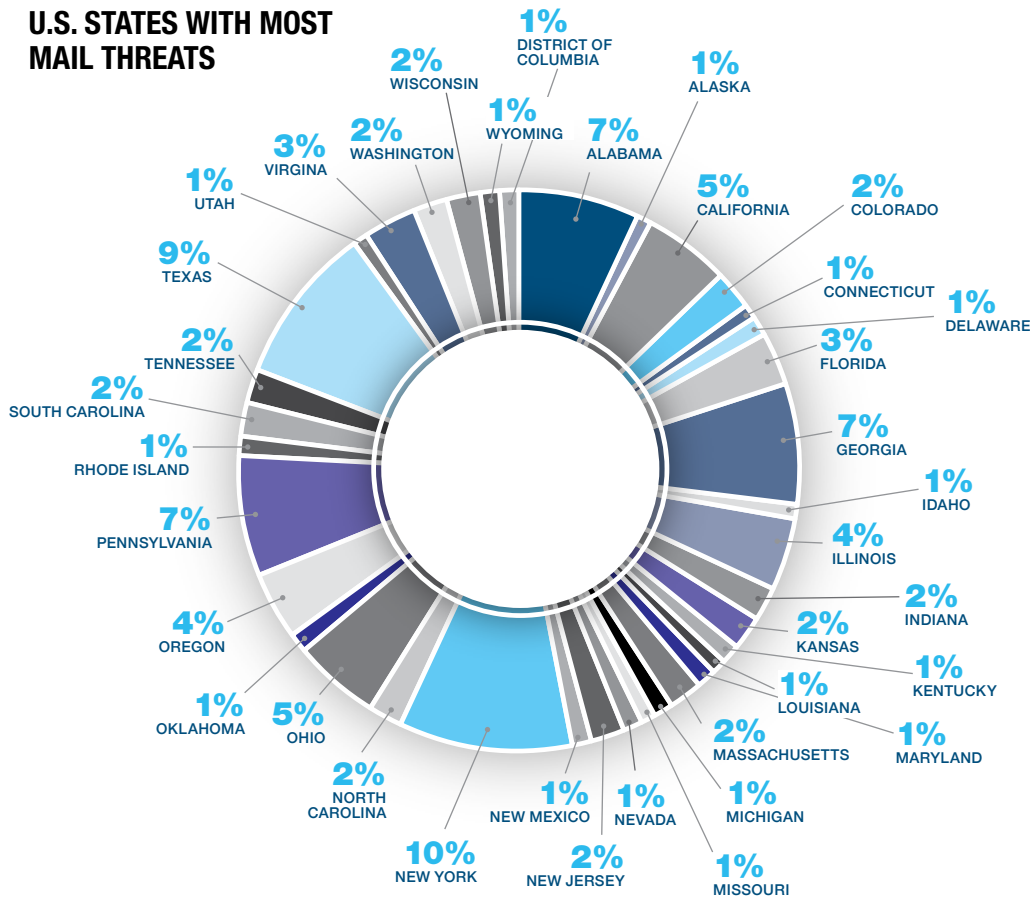
As noted, 2021 saw a significant increase in racist and extremist mail events — everything from simple insulting language to direct threats of individuals and groups. Unfortunately, almost every minority group was targeted with several notable increases due to the reaction from the pandemic. As with any threat of this nature, mail threats can be expected to escalate. Recipients who ignore or dispose of materials might leave authorities with less recourse should the sender become more aggressive. Instead, reports should be generated with all possible information captured to protect both the employees and the organization as a whole, and more importantly, communicate the extent of the problem to better inform measures to mitigate these threats.



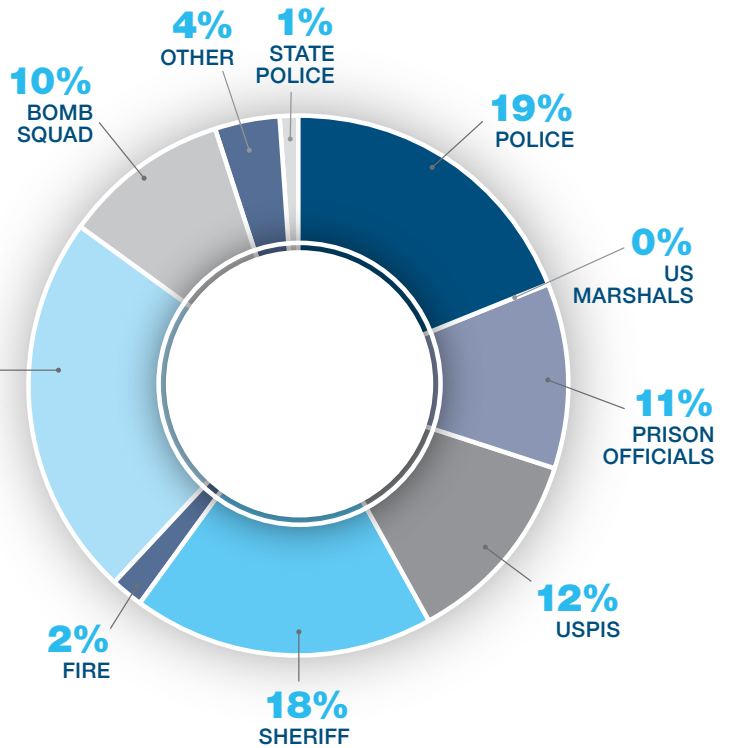
2021 Threat Data in More Detail



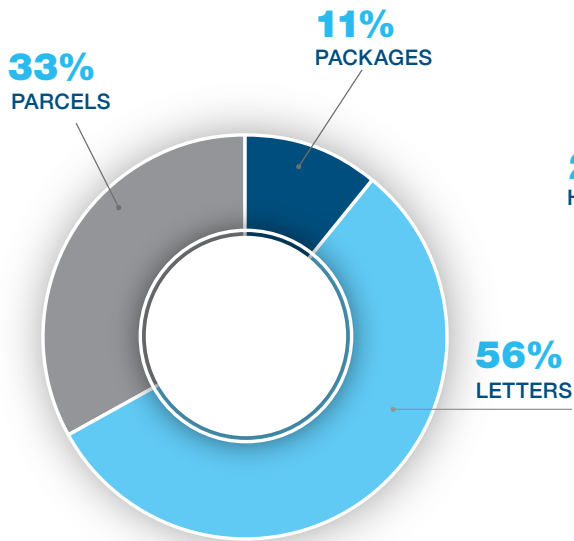
U.S. STATES WITH MOST MAIL THREATS



PRIMARY RESPONDER



DELIVERY METHOD

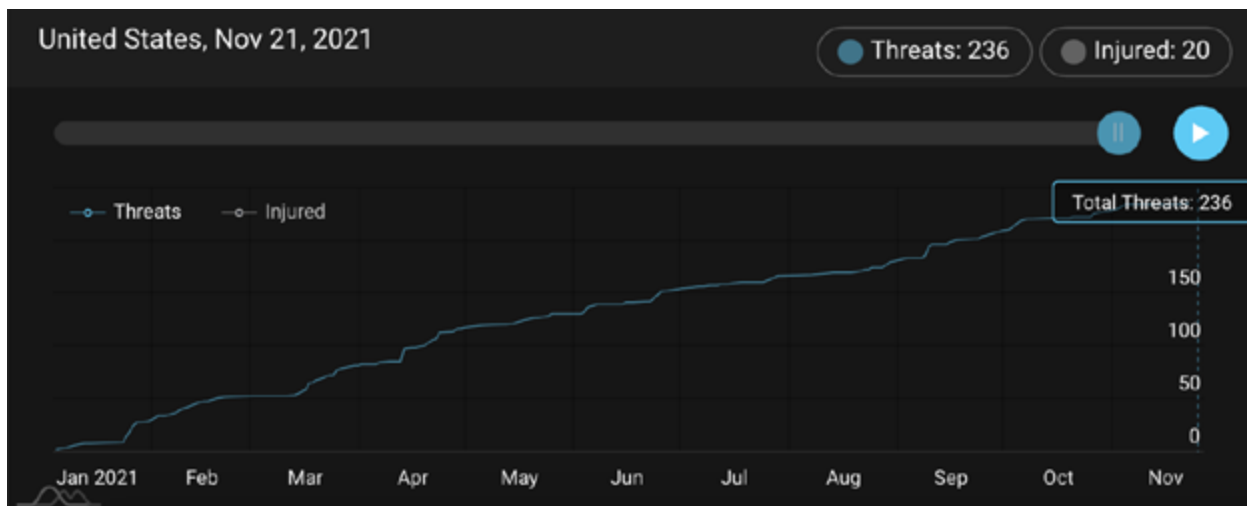
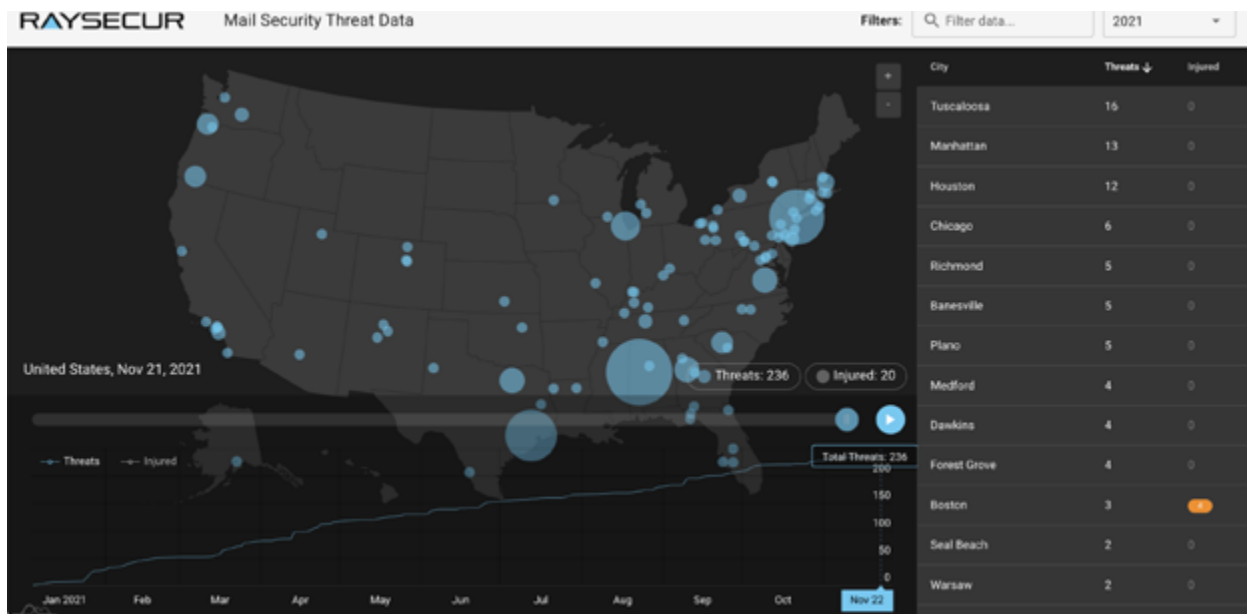


Threat Data Center

The TDC is an informational product prepared by RaySecur utilizing open-source reporting to present a comprehensive view of the state of mail-borne threats.

This interactive and dynamic map provides up-to-date information on mail threats across the United States.

For additional information on this and other mail security solutions, contact RaySecur CSO Will Plummer, will@raysecur.com. Try out the Threat Data Center map for yourself at RaySecur.com/Mail-Threat-Data/



References

- 2020 United States Postal Inspection Service (USPIS) annual report and 2020 United States Bomb Data Center (USBDC) Explosives Incident Report (EIR)
<https://www.uspis.gov/wp-content/uploads/2021/07/FY2020-annual-report-web-FINAL.pdf>
- Postal Facts
<https://facts.usps.com/inspection-service/>
- 2020 United States Postal Inspection Service (USPIS) Annual Report.
<https://www.uspis.gov/wp-content/uploads/2021/07/FY2020-annual-report-web-FINAL.pdf>
- 2020 United States Bomb Data Center (USBDC) Explosives Incident Report (EIR)
<https://www.atf.gov/file/155141/download>
- Guide to Mail Center Security
<https://about.usps.com/publications/pub166.pdf>
- Center for the Protection of National Infrastructure
<https://www.cpni.gov.uk/>
- USPS Postal Explorer, Business Mail 101
<https://pe.usps.com/businessmail101?ViewName=Parcels>
- USPIS 2020 Annual Report.
<https://www.uspis.gov/wp-content/uploads/2021/07/FY2020-annual-report-web-FINAL.pdf>
- Global Terrorism Database, National Consortium for the Study of Terrorism and Response to Terroris
<https://www.start.umd.edu/gtd/>
- Letter addressed to the pope with three bullets inside is sent to vatican
<https://metro.co.uk/2021/08/09/popefrancis-receives-bullets-in-envelope-deaththreat-15061637/>
- The Guardian, Three letter bombs sent to German firms may be linked, say investigators
<https://www.theguardian.com/world/2021/feb/19/letter-bombs-sent-to-german-firms-lidl-hipp-may-be-linked>
- UK AstraZeneca vaccine plant says production unaffected by suspect package
<https://www.reuters.com/article/uk-health-coronavirus-britain-astra-inci/uk-astrazeneca-vaccine-plant-says-production-unaffected-by-suspect-package-idUSKBN29W1JC>
- WGN9 Chicago, Authorities probe Obama, VP Harris hate mail sent to Chicago's DuSable Museum
<https://wgntv.com/news/chicago-news/authorities-probe-threatening-mail-sent-to-chicagos-dusable-museum/>
- Forbes, Black Hat USA 2019: IBM X-Force Red Reveals New 'Warshipping' Hack To Infiltrate Corporate Networks
<https://www.forbes.com/sites/jeanbaptiste/2019/08/08/black-hat-usa-2019-ibm-x-force-red-reveals-new-warshipping-hack-to-infiltrate-corporate-networks/?sh=299d37f604f5>
- The New York Times, Fauci on What Working for Trump Was Really Like
<https://www.nytimes.com/2021/01/24/health/fauci-trump-covid.html>
- The Guardian, Three letter bombs sent to German firms may be linked, say investigators
<https://www.theguardian.com/world/2021/feb/19/letter-bombs-sent-to-german-firms-lidl-hipp-may-be-linked>
- NBC News, Suspicious package with white powder sent to Sen. Rand Paul's Kentucky home
<https://www.nbcnews.com/politics/congress/suspicious-package-white-powder-sent-sen-rand-paul-s-kentucky-n1268442>
- WGN9 Chicago, Authorities probe Obama, VP Harris hate mail sent to Chicago's DuSable Museum
<https://wgntv.com/news/chicago-news/authorities-probe-threatening-mail-sent-to-chicagos-dusable-museum/>
- South China Morning Post, Bomb squad mobilized, courts partially evacuated after 2 Hong Kong judges receive letters containing dangerous chemical
<https://www.scmp.com/news/hong-kong/law-and-crime/article/3156211/bomb-squad-mobilised-2-more-hong-kong-courts-receive>
- Myanmar Now, Bomb explodes at CID headquarters in Naypyitaw
<https://www.myanmar-now.org/en/news/bomb-explodes-at-cid-headquarters-in-naypyitaw>
- St. Louis Post-Dispatch, Clayton Police FBI Respond to Threatening Letter with White Powder
https://www.stltoday.com/news/local/crime-and-courts/clayton-police-fbi-respond-to-threatening-letter-with-white-powder/article_aaef4fef-d4d3-5a04-99d2-a463d289e5e2.html
- The Columbian, Oregon man pleads guilty to mailing cards with pesticide in them
<https://www.columbian.com/news/2021/feb/09/oregon-man-pleads-guilty-to-mailing-cards-with-pesticide-in-them/>
- Daily Voice, Residents Become Dizzy After Opening "Suspicious" Package in Hudson Valley
<https://dailyvoice.com/new-york/eastdutchess/police-fire/residents-become-dizzy-after-opening-suspicious-package-in-hudson-valley/805447/>
- Click 2 Houston.com, FBI, Postal Inspector looking into suspicious mail sent to Houston Jewelry
<https://www.click2houston.com/news/local/2021/04/14/fbi-us-postal-inspector-looking-into-suspicious-mail-sent-to-houston-jewelry>
- Daily Mail.com, Tennessee nurse, 37, is charged with mailing blood-stained sanitary napkin and dog feces to her husband's ex-wife
<https://www.heraldmillmedia.com/story/news/local/2021/07/07/inmate-posing-another-charged-threatening-bomb-judges/7874369002/>
- Inmate Posing Another Charged Threatening Bomb Judges
<https://www.heraldmillmedia.com/story/news/local/2021/07/07/inmate-posing-another-charged-threatening-bomb-judges/7874369002/>
- 7 News, Four officers injured in inmate attack at Cape Vincent prison, union says
<https://www.wnnytv.com/2021/08/26/4-officers-injured-inmate-attack-cape-vincentprison-union-says/>
- KTVB7, Idaho lawmakers receive threatening letters over wolf law
<https://www.ktvb.com/article/news/politics/idaho-lawmakers-receive-threatening-letters-over-wolf-law/277-c6e0fa87-f46b-4b21-9526-a36d7d5f0aca>
- Scene Cleared after 'suspicious' package found at UTRGV building in Edinburg
<https://www.krgv.com/news/scene-cleared-after-suspicious-package-found-at-utrgv-building-in-edinburg/>
- USA Today, US Rep. Ilhan Omar's Capitol Hill office receives package with "suspicious substance"
<https://www.usatoday.com/story/news/politics/2021/10/26/rep-ilhan-omars-office-gets-package-suspicious-substance/8559191002/>
- Fox News, "Chinese Zodiac Killer" sends letters to New York TV stations
<https://www.foxnews.com/us/chinese-zodiac-killer-sends-letters-to-new-york-tv-stations>

The Standard In Mail Security

About RaySecur:

RaySecur is a security imaging company revolutionizing mail and package scanning. The MailSecur™ is the world's first DHS Safety Act-designated T-ray scanner, providing real-time, 4D imaging, in an all-in-one desktop mail security solution. T-ray technology is safe, requires no licenses or permits, and detects all nine types of postal threats identified by the Department of Homeland Security (DHS) - unlike X-ray which uses harmful radiation and detects only three of the nine DHS-listed threats. MailSecur is supported by EODSecur™ service, providing 24x365 on-call threat response by trained military Explosive Ordnance Disposal (EOD) professionals, in addition to supporting end-user training and standard operating procedures.

RAYSECUR™
THE STANDARD IN MAIL SECURITY

raysecur.com | 617-855-9938 | info@raysecur.com