

# **HB946 Porch piracy.pdf**

Uploaded by: cailey locklair

Position: FAV



## HB946 Criminal Law - Theft - Mail and Packages (Porch Piracy Act of 2024)

February 20<sup>th</sup>, 2024

### SUPPORT

**Background:** Prohibiting the theft of mail or packages from intended recipients.

**Comments:** As an increasing number of consumers add online commerce to their retail experience, loss prevention statutes need to be modernized to protect purchases delivered through this channel. We believe specific porch piracy statutes help accomplish that objective.

Customers rely on retailers and retail delivery partners to deliver packages on time, intact, and securely. When porch piracy prevents customers from having a good retail experience, it erodes customer trust.

We have heard from law enforcement that lack of clear and consistently applicable statutes under which to charge porch pirates is an obstacle in combating the problem. Law enforcement entities have specifically pointed to unclear and limited statutes under which to charge and prosecute porch pirates as a barrier to successful deterrence of porch piracy. As a result, package theft is often committed by repeat offenders, harming the consumer experience, undermining customer trust and costing the retailer.

At the federal level, under 18 U.S.C. § 1708, mail theft is committed by one who “steals, takes, or abstracts, ... from or out of any mail, post office, or station thereof, letter box, mail receptacle, or any mail route or other authorized depository for mail matter, or from a letter or mail carrier, any ... package ... or abstracts or removes from any such ... package ... any article or thing contained therein.” This law has been interpreted by the courts to apply only to mail carried by the United States Postal Service (USPS), rather than private carriers.

In crafting a state mail theft statute, it is helpful to consider holistic language that includes every day package delivery by all carries, not just postal items delivered by USPS. Thus, we urge a favorable report on this legislation.

**HB 0946 - MBA - FAV - GR24.pdf**

Uploaded by: Evan Richards

Position: FAV



**HB 946 – Criminal Law – Theft – Mail and Packages (Porch Piracy Act of 2024)**

**Committee:** House Judiciary Committee

**Date:** February 20, 2024

**Position:** Favorable

The Maryland Bankers Association (MBA) **SUPPORTS** HB 946. This legislation prohibits the theft of mail and packages from their intended recipients. Passing this legislation will provide additional tools to prosecute those who prevent Marylanders from receiving their mail, which can include items like financial statements and checks.

Despite a decline of check usage across the country, criminals are increasingly targeting the mail to commit check fraud. When criminals steal a check, they can “wash” the check with chemicals to remove ink, allowing them to change the payee’s name and the dollar amount and cash the check with a depository institution. According to FinCEN, depository institutions filed over 680,000 Suspicious Activity Reports (SARs) on potential check fraud last year, which is a 130% increase in filings from 2020.

This sophisticated check fraud is a serious issue, and Maryland banks are working to implement innovative solutions that counter check fraud, including deposit reviews, fraud detection tools, hold policies, and increased customer and employee education.

Maryland banks have seen a surge of mail-theft related check fraud. HB 946 arms prosecutors with additional tools to help protect Maryland residents.

Accordingly, MBA urges issuance of a **FAVORABLE** report on HB 946.

*The Maryland Bankers Association (MBA) represents FDIC-insured community, regional, and national banks, employing more than 26,000 Marylanders and holding more than \$209 billion in deposits in over 1,200 branches across our State. The Maryland banking industry serves customers across the State and provides an array of financial services including residential mortgage lending, business banking, estates and trust services, consumer banking, and more.*

Submitted by: Evan Richards  
Senior Policy & Political Strategist, Maryland Bankers Association  
186 Duke of Gloucester Street  
Annapolis, MD 21401



# FinCEN

# ALERT

FIN-2023-Alert003

February 27, 2023

## FinCEN Alert on Nationwide Surge in Mail Theft-Related Check Fraud Schemes Targeting the U.S. Mail

### Suspicious Activity Report (SAR) Filing Request:

FinCEN requests that financial institutions reference this alert in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the key term “FIN-2023-MAILTHEFT” and marking the check box for check fraud (SAR Field 34(d)).

In light of a nationwide surge in check fraud schemes targeting the U.S. Mail<sup>1</sup> (hereinafter “mail theft-related check fraud”), the Financial Crimes Enforcement Network (FinCEN) is issuing this alert to financial institutions<sup>2</sup> to be vigilant in identifying and reporting such activity. Mail theft-related check fraud generally pertains to the fraudulent negotiation of checks stolen from the U.S. Mail. Fraud, including check fraud, is the largest source of illicit proceeds in the United States and represents one of the most significant money laundering threats to the United States, as highlighted in the U.S. Department of the Treasury’s most recent National Money Laundering Risk Assessment and

National Strategy for Combatting Terrorist and other Illicit Financing.<sup>3</sup> Fraud is also one of the anti-money laundering/countering the financing of terrorism (AML/CFT) National Priorities.<sup>4</sup>

FinCEN is issuing this alert in close collaboration with the United States Postal Inspection Service (USPIS)<sup>5</sup> to ensure that SARs filed by financial institutions appropriately identify and report suspected check fraud schemes that may be linked to mail theft in the United States. This alert provides an overview of a recent surge in mail theft-related check fraud, highlights select red flags to assist financial institutions in identifying and reporting suspicious activity, and reminds financial institutions of their reporting requirements under the Bank Secrecy Act (BSA).

The information contained in this alert is derived from FinCEN’s analysis of BSA data, open-source reporting, and information provided by law enforcement partners.

1. “U.S. Mail” is a registered trademark of the United States Postal Service (USPS) and includes all mail distributed and delivered through and by the Postal Service. This includes First-Class Mail such as mailed letters, cards, or other correspondence, which may contain checks, money orders, personal identifiable information, and credit cards/debit cards.
2. See 31 U.S.C. § 5312(a)(2); 31 CFR § 1010.100(t).
3. See U.S. Department of the Treasury, “[National Money Laundering Risk Assessment](#)” (Feb. 2022), at pp. 6-7; U.S. Department of the Treasury, “[National Strategy for Combatting Terrorist and Other Illicit Financing](#)” (May 2022), at p. 27.
4. See FinCEN, “[Anti-Money Laundering and Countering the Financing of Terrorism National Priorities](#)” (June 30, 2021).
5. The USPIS is the law enforcement, crime prevention, and security arm of the USPS. Postal Inspectors are federal law enforcement agents who have broad authority to investigate violations of federal law that have a nexus to the U.S. Mail and USPS, including mail theft and associated financial crimes. USPIS is one of several federal agencies with authority to investigate the laundering of illicit proceeds. For more information, visit [United States Postal Inspection Service \(uspis.gov\)](#). See also USPIS, “[Annual Report 2021](#)” (July 12, 2022).

## Emerging Trends in Mail Theft-Related Check Fraud Schemes

Despite the declining use of checks in the United States,<sup>6</sup> criminals have been increasingly targeting the U.S. Mail since the COVID-19 pandemic to commit check fraud.<sup>7</sup> The United States Postal Service (USPS) delivers nearly 130 billion pieces of U.S. Mail every year to over 160 million residential and business addresses across the United States.<sup>8</sup> From March 2020 through February 2021, the USPIS received 299,020 mail theft complaints, which was an increase of 161 percent compared with the same period a year earlier.<sup>9</sup> BSA reporting for check fraud has also increased in the past three years. In 2021, financial institutions filed more than 350,000 SARs to FinCEN to report potential check fraud, a 23 percent increase over the number of check fraud-related SARs filed in 2020. This upward trend continued into 2022, when the number of SARs related to check fraud reached over 680,000, nearly double the previous year's amount of filings.<sup>10</sup>

### Mail Theft Risks and Vulnerabilities

Criminals committing mail theft-related check fraud generally target the U.S. Mail in order to steal personal checks, business checks, tax refund checks, and checks related to government assistance programs, such as Social Security payments and unemployment benefits. Criminals will generally steal all types of checks in the U.S. Mail as part of a mail theft scheme, but business checks may be more valuable because business accounts are often well-funded and it may take longer for the victim to notice the fraud. There have been cases of Postal Service employees stealing checks at USPS sorting and distribution facilities.<sup>11</sup> However, according to USPIS, mail theft-related check fraud is increasingly committed by non-USPS employees, ranging from individual fraudsters to organized criminal groups comprised of the organizers of the criminal scheme, recruiters, check washers, and money mules.

- 
6. According to analysts at the Federal Reserve Bank of Atlanta, “[f]rom 2015 to 2018, the proportion of consumers who state checks are their preferred payment method declined by 23 percent for bills and 8 percent for purchases.” See Claire Greene, Marcin Hitzenko, Brian Prescott, and Oz Shy, Research Data Reports, [“U.S. Consumers’ Use of Personal Checks: Evidence from a Diary Survey”](#) Federal Reserve Bank of Atlanta (Feb. 2020), at p. 1. Concurrently, estimates from the Board of Governors of the Federal Reserve illustrate that, on average, the dollar amount per commercial check is increasing annually. See Board of Governors of the Federal Reserve System, [Commercial Checks Collected Through the Federal Reserve—Quarterly Data](#).
  7. FinCEN previously issued an advisory to alert financial institutions to check fraud and other financial crimes involving Economic Impact Payments authorized by the Coronavirus Aid, Relief, and Economic Security (CARES) Act and the Coronavirus Response and Relief Supplemental Appropriations Act of 2021. See FinCEN, [“Advisory on Financial Crimes Targeting COVID-19 Economic Impact Payments”](#) (Feb. 24, 2021).
  8. See USPIS, “Annual Report 2021,” *supra* footnote 5, at p. 19.
  9. See USPS Office of Inspector General, Audit Report, [“U.S. Postal Inspection Service Pandemic Response to Mail Fraud and Mail Theft”](#) (May 20, 2021), at p. 5.
  10. See [FinCEN SAR Stats](#). This statistic includes all SARs with box 34(d), *check fraud*, marked and is not indicative of specifically mail theft-related check fraud.
  11. See U.S. Department of Justice (DOJ), Press Release, [“Multiple U.S. Postal Service Employees and Others Arrested for \\$1.3 Million Fraud and Identity Theft Scheme”](#) (Sept. 29, 2022); DOJ, Press Release, [“Queens Postal Workers Charged with Bribery Scheme and Theft of Mail Linked to COVID-19 Benefits Fraud”](#) (Aug. 12, 2022).

**Check Washers:** Check washing involves the use of chemicals to remove the original ink on a check to replace the payee and often the dollar amount. Fraudsters may also copy and print multiple washed checks for future use or to sell to third-party criminals.<sup>12</sup>

**Money Mules:** A money mule is a person (whether witting or unwitting) who transfers or moves illicit funds at the direction of or on behalf of another.<sup>13</sup>

These criminals, located throughout the country, target USPS blue collection boxes, unsecured residential mailboxes, and privately owned cluster box units at apartment complexes, planned neighborhoods, and high-density commercial buildings. Mail theft can occur through forced entry or the use of makeshift fishing devices,<sup>14</sup> and increasingly involves the use of authentic or counterfeit USPS master keys, known as Arrow Keys. Arrow Keys open USPS blue collection boxes and cluster box units within a geographic area, and a number of recent cases involve organized criminals violently targeting USPS mail carriers with the intent of stealing Arrow Keys.<sup>15</sup> There have also been cases of corrupt Postal Service employees who unlawfully provide Arrow Keys to criminal actors to facilitate mail theft.<sup>16</sup> Illicit actors may also copy and sell stolen Arrow Keys to third-party fraudsters on the dark web and through encrypted social media platforms in exchange for convertible virtual currency.

## Typologies of Mail Theft-Related Check Fraud and Associated Money Laundering







After stealing checks from the U.S. Mail, fraudsters and organized criminal groups may alter or “wash” the checks, replacing the payee information with their own or fraudulent identities or with business accounts that the criminals control. During check washing, these illicit actors also often increase the dollar amount on the check, sometimes by hundreds or thousands of dollars. Washed checks may also be copied, printed, and sold to third-party fraudsters on the dark web and encrypted social media platforms in exchange for convertible virtual currency. In some cases,

12. See USFIS, Scam Article, [Check Washing](#) (Sept. 22, 2022).
13. See USFIS, Scam Article, [Money Mule](#) (June 1, 2022); DOJ, [Money Mule Initiative](#); Federal Bureau of Investigation (FBI) Internet Crime Complaint Center, Public Service Announcement, “[Money Mules: A Financial Crisis](#)” (Dec. 3, 2021); FBI, [Money Mules](#); see also United States Secret Service, Press Release, “[Georgia Man Sentenced in Bank Fraud Scheme that Exploited Homeless Rhode Islanders](#)” (Feb. 16, 2022).
14. Fishing devices are makeshift items, usually with an adhesive substance applied, which have the purpose of adhering to U.S. Mail to facilitate the surreptitious removal of the U.S. Mail from a blue collection box.
15. See DOJ, Press Release, “[Tampa Man Found Guilty of Armed Robbery of a Postal Carrier](#)” (Jan. 27, 2023); DOJ, Press Release, “[Three Philadelphia-Area Men Charged in Connection with USPS Arrow Key, Mail Theft from Blue Collection Boxes](#)” (Oct. 4, 2022); DOJ, Press Release, “[Four Defendants Facing Federal Charges for Mail Theft and Possession of United States Postal Service Keys](#),” (July 29, 2022); DOJ, Press Release, “[Three Philadelphia-Area Men Charged in Connection with Scheme to Wash and Alter Checks Stolen from USPS Collection Boxes](#)” (July 25, 2022); DOJ, Press Release, “[Nicaraguan Man Sentenced to More Than 11 Years in Prison for 2-Week Robbery Spree of U.S. Postal Service Mail Carriers](#)” (July 14, 2022); DOJ, Press Release, “[Sacramento County Man Sentenced to 10 Years in Prison for Armed Robbery of a U.S. Mail Carrier and Bank Fraud](#)” (Mar. 1, 2022); DOJ, Press Release, “[Passaic County Man Charged with Attempted Robbery of Two U.S. Postal Service Employees](#)” (Feb. 9, 2022).
16. See DOJ, Press Release, “[Postal Worker Pleads Guilty to Aiding and Abetting Mail Theft in Liverpool](#)” (Feb. 26, 2021).

victim checks are also counterfeited using routing and account information from the original, stolen check.<sup>17</sup> Illicit actors may cash or deposit checks in person at financial institutions, through automated teller machines (ATMs), or via remote deposit into accounts they control, and which they often open specifically for the check fraud schemes. Criminals may also rely on money mules and their pre-existing accounts to deposit fraudulent checks.<sup>18</sup> Regardless, once the checks are deposited, the illicit actors often rapidly withdraw the funds through ATMs or wire them to other accounts that they control to further obfuscate their ill-gotten gains. The criminals may further exploit the victims by using personal identifiable information found in the stolen mail for future fraud schemes such as credit card fraud or credit account fraud.<sup>19</sup>

## Financial Red Flags Relating to Mail Theft-Related Check Fraud

FinCEN, in coordination with USPIS, has identified red flags to help financial institutions detect, prevent, and report suspicious activity connected to mail theft-related check fraud, many of which overlap with red flags for check fraud in general. As no single red flag is determinative of illicit or suspicious activity, financial institutions should consider the surrounding facts and circumstances, such as a customer’s historical financial activity, whether the transactions are in line with prevailing business practices, and whether the customer exhibits multiple red flags, before determining if a behavior or transaction is suspicious or otherwise indicative of mail theft-related check fraud. In line with their risk-based approach to compliance with the BSA, financial institutions are also encouraged to perform additional due diligence where appropriate.

-  1 Non-characteristic large withdrawals on a customer’s account via check to a new payee.
-  2 Customer complains of a check or checks stolen from the mail and then deposited into an unknown account.
-  3 Customer complains that a check they mailed was never received by the intended recipient.
-  4 Checks used to withdraw funds from a customer’s account appear to be of a noticeably different check stock than check stock used by the issuing bank and check stock used for known, legitimate transactions.
-  5 Existing customer with no history of check deposits has new sudden check deposits and withdrawal or transfer of funds.
-  6 Non-characteristic, sudden, abnormal deposit of checks, often electronically, followed by rapid withdrawal or transfer of funds.

17. See USPIS, Scam Article, [Check Fraud](#) (May 1, 2019).

18. In the case of mail theft-related check fraud, money mules are generally younger in age and are witting accomplices in the scheme. In certain cases, criminal organizations prey upon homeless individuals and addicts by soliciting them as money mules and giving them a small portion of the cashed checks.

19. See generally DOJ, Press Release, “[Repeat Offender on Supervised Release Admits to Stealing Mail and Pleads Guilty to Wire Fraud](#)” (June 7, 2022).



- 7 Examination of suspect checks reveals faded handwriting underneath darker handwriting, giving the appearance that the original handwriting has been overwritten.
- 8 Suspect accounts may have indicators of other suspicious activity, such as pandemic-related fraud.<sup>20</sup>
- 9 New customer opens an account that is seemingly used only for the deposit of checks followed by frequent withdrawals and transfer of funds.
- 10 A non-customer that is attempting to cash a large check or multiple large checks in-person and, when questioned by the financial institution, provides an explanation that is suspicious or potentially indicative of money mule activity.

### Mail Theft-Related Check Fraud Reporting Hotline for Victims

In addition to filing a SAR, as applicable, financial institutions should refer their customers who may be victims of mail theft-related check fraud to the USPIS at 1-877-876-2455 or <https://www.uspis.gov/report> to report the incident.

### USPIS Tips to Prevent Mail Theft

FinCEN recommends as a best practice that financial institutions refer their customers to [www.uspis.gov/tips-prevention/mail-theft](http://www.uspis.gov/tips-prevention/mail-theft) for tips from the USPIS on how to protect against mail theft.

If customers appear to be a victim of a theft involving USPS money orders, refer them to <https://www.usps.com/shop/money-orders.htm> for guidance on how to replace a lost or stolen money order.

20. See FinCEN, [“Advisory on Financial Crimes Targeting COVID-19 Economic Impact Payments”](#) (Feb. 24, 2021); DOJ, Press Release, [“Queens Postal Workers Charged with Bribery Scheme and Theft of Mail Linked to COVID-19 Benefits Fraud”](#) (Aug. 12, 2022); DOJ, Press Release, [“Defendant Sentenced for Mail Theft and Possession of Stolen Mail, including Stimulus Checks”](#) (June 28, 2021).

## Reminder of Relevant BSA Obligations and Tools for U.S. Financial Institutions

### *Suspicious Activity Reporting Other Relevant BSA Reporting*

#### *USA PATRIOT ACT Section 314(b) Information Sharing Authority*

### Suspicious Activity Reporting

A financial institution is required to file a SAR if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves funds derived from illegal activity; is intended or conducted to disguise funds derived from illegal activity; is designed to evade regulations promulgated under the BSA; lacks a business or apparent lawful purpose; or involves the use of the financial institution to facilitate criminal activity.<sup>21</sup> All statutorily defined financial institutions may voluntarily report suspicious transactions under the existing suspicious activity reporting safe harbor.<sup>22</sup>

When a financial institution files a SAR, it is required to maintain a copy of the SAR and the original or business record equivalent of any supporting documentation for a period of five years from the date of filing the SAR.<sup>23</sup> Financial institutions must provide any requested documentation supporting the filing of a SAR upon request by FinCEN or an appropriate law enforcement or supervisory agency.<sup>24</sup> When requested to provide supporting documentation, financial institutions should take special care to verify that a requestor of information is, in fact, a representative of FinCEN or an appropriate law enforcement or supervisory agency. A financial institution should incorporate procedures for such verification into its BSA compliance or AML program. These procedures may include, for example, independent employment verification with the requestor's field office or face-to-face review of the requestor's credentials.

### SAR Filing Instructions

FinCEN requests that financial institutions indicate a connection between the suspicious activity being reported and the activities highlighted in this alert by including the key term "**FIN-2023-MAILTHEFT**" in SAR field 2 ("Filing Institution Note to FinCEN"), as well as in the narrative, and by selecting **SAR Field 34(d) (check fraud)**. Financial institutions may highlight additional advisory or alert keywords in the narrative, if applicable.

21. See 31 CFR §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.320.

22. See 31 U.S.C. § 5318(g)(3). Financial institutions may report suspicious transactions regardless of amount involved and still take advantage of the safe harbor.

23. See 31 CFR §§ 1020.320(d), 1021.320(d), 1022.320(c), 1023.320(d), 1024.320(c), 1025.320(d), 1026.320(d), 1029.320(d), 1030.320(d).

24. *Id.* See also FinCEN, "[Suspicious Activity Report Supporting Documentation](#)" (June 13, 2007).

*Financial institutions wanting to expedite their report of suspicious transactions that may relate to the activity noted in this alert should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day).<sup>25</sup>*

Financial institutions should include any and all available information relating to the account and locations involved in the reported activity, identifying information and descriptions of any legal entities or arrangements involved and associated beneficial owners, and any information about related persons or entities involved in the activity. Financial institutions also should provide any and all available information regarding other domestic and foreign financial institutions involved in the activity; where appropriate, financial institutions should consider filing a SAR jointly on shared suspicious activity.<sup>26</sup>

### **Other Relevant BSA Reporting Requirements**

Financial institutions and other entities or persons also may have other relevant BSA reporting requirements to provide information in connection with the subject of this alert. These include obligations related to the Currency Transaction Report (CTR),<sup>27</sup> Report of Cash Payments Over \$10,000 Received in a Trade or Business (Form 8300),<sup>28</sup> Report of Foreign Bank and Financial Accounts (FBAR),<sup>29</sup> Report of International Transportation of Currency or Monetary Instruments (CMIR),<sup>30</sup> Registration of Money Services Business (RMSB),<sup>31</sup> and Designation of Exempt Person (DOEP).<sup>32</sup> These standard reporting requirements may not have an obvious connection to illicit finance, but may ultimately prove highly useful to law enforcement.

- 
25. The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local area law enforcement officials.
  26. See 31 CFR §§ 1020.320(e)(1)(ii)(A)(2)(i), 1021.320(e)(1)(ii)(A)(2), 1022.320(d)(1)(ii)(A)(2), 1023.320(e)(1)(ii)(A)(2)(i), 1024.320(d)(1)(ii)(A)(2), 1025.320(e)(1)(ii)(A)(2), 1026.320(e)(1)(ii)(A)(2)(i), 1029.320(d)(1)(ii)(A)(2), 1030.320(d)(1)(ii)(A)(2).
  27. A report of each deposit, withdrawal, exchange of currency, or other payment or transfer, by, through, or to a financial institution that involves a transaction in currency of more than \$10,000. Multiple transactions may be aggregated when determining whether the reporting threshold has been met. See 31 CFR §§ 1010.310-313, 1020.310-313, 1021.310-313, 1022.310-313, 1023.310-313, 1024.310-313, and 1026.310-313.
  28. A report filed by a trade or business that receives currency in excess of \$10,000 in one transaction or two or more related transactions. The transactions are required to be reported on a joint FinCEN/Internal Revenue Service form when not otherwise required to be reported on a CTR. See 31 CFR § 1010.330; 31 CFR § 1010.331. A Form 8300 also may be filed voluntarily for any suspicious transaction, even if the total amount does not exceed \$10,000.
  29. A report filed by a U.S. person that has a financial interest in, or signature or other authority over, foreign financial accounts with an aggregate value exceeding \$10,000 at any time during the calendar year. See 31 CFR § 1010.350; FinCEN Form 114.
  30. A form filed to report the transportation of more than \$10,000 in currency or other monetary instruments into or out of the United States. See 31 CFR § 1010.340.
  31. A form filed to register a money services business (MSB) with FinCEN, or to renew such a registration. See 31 CFR § 1022.380.
  32. A report filed by banks to exempt certain customers from currency transaction reporting requirements. See 31 CFR § 1010.311.

## Form 8300 Filing Instructions

When filing a Form 8300 involving a suspicious transaction relevant to this alert, FinCEN requests that the filer select *Box 1b* (“suspicious transaction”) and include the key term “FIN-2023-MAILTHEFT” in the “Comments” section of the report.

## Information Sharing

Information sharing among financial institutions is critical to identifying, reporting, and preventing mail theft-related check fraud or other illicit financial activity. Financial institutions and associations of financial institutions sharing information under the safe harbor authorized by section 314(b) of the USA PATRIOT Act are reminded that they may share information with one another regarding individuals, entities, organizations, and countries suspected of possible terrorist financing or money laundering.<sup>33</sup> FinCEN strongly encourages such voluntary information sharing.

## For Further Information

Questions regarding the contents of this alert should be addressed to the FinCEN Regulatory Support Section at [frc@fincen.gov](mailto:frc@fincen.gov).

---

33. See FinCEN, “[Section 314\(b\) Fact Sheet](#)” (Dec. 2020).

**Letter Supporting Package Theft Bill 946 2-2024.pd**

Uploaded by: Jason Shoemaker

Position: FAV



J. CHARLES SMITH, III  
STATE'S ATTORNEY

CIRCUIT COURT DIVISION  
301-600-1523

DISTRICT COURT DIVISION  
301-600-2573

CHILD SUPPORT DIVISION  
301-600-1538

JUVENILE DIVISION  
301-600-2980

**STATE'S ATTORNEY FOR FREDERICK COUNTY**

KIRSTEN N. BROWN  
DEPUTY STATE'S ATTORNEY

County Courthouse  
100 West Patrick Street  
Frederick, Maryland 21701

[www.statesattorney.us](http://www.statesattorney.us)

February 16, 2024

The Honorable Luke Clippinger  
Chairperson, House Judiciary Committee  
House Office Building, Room 100  
6 Bladen Street  
Annapolis, MD 21401

Dear Chair Clippinger and Members of the Judiciary Committee:

On behalf of the Maryland State's Attorney's Association, and the Frederick County State's Attorney's Office, I write in support of House Bill 946 which has the intended purpose of prohibiting the theft of mail or packages from intended recipients.

Whether it be the news or cases coming across my desk, this crime is at epidemic levels. It may be one of the few remaining universal joys to order an item online, track its shipment and delivery, and then locate that item at your house. And, perhaps, as equally disdained as ordering these items for delivery is loved, is failing to find your package, and then realizing it was stolen. With the increase of package delivery as a means for Americans, including Marylanders, to obtain the items they want and need, the criminal enterprise of engaging in the theft of those packages has spiked.

Cases I have reviewed have involved thieves watching for delivery trucks, following delivery trucks, and arranging for delivery of items to the victim, all with the intention of intercepting and stealing packages before the victim takes possession of it.

While home surveillance systems have facilitated the identification and apprehension of these culprits, the current theft law structure connects the level of consequence for the crime to the value of the item(s) stolen. While there are certainly circumstances where the amount stolen reaches into the thousands of dollars, we are typically seeing these thefts yielding under \$1,500.00 in value. Under Maryland Code Annotated, Criminal Law section 7-104, for a first offense, an offender is only facing 6 months and/or a fine of \$500.

The epidemic level of this offense, as well as the frustration incurred upon the victim when this crime occurs, warrants a potential consequence greater than 6 months in jail. I particularly appreciate the clear and simple prohibition and penalty wording of the bill. A thief who steals a package from the exterior of a victim's residence has engaged in a simple crime. The amount of burden and effort on behalf of the prosecution to litigate this offense should be as streamlined as possible. This bill does that.

Thank you for the opportunity to provide support for this bill and I urge this Committee to issue a favorable report on House Bill 946.

Sincerely,

A handwritten signature in black ink, appearing to read "Jason S. Shoemaker". The signature is fluid and cursive, with the first name "Jason" being the most prominent.

Jason S. Shoemaker,  
Chief, Economic Crimes Unit

# **MOPD Unfavorable Testimony HB946.pdf**

Uploaded by: Natasha Khalfani

Position: UNF





**NATASHA DARTIGUE**  
PUBLIC DEFENDER

**KEITH LOTRIDGE**  
DEPUTY PUBLIC DEFENDER

**MELISSA ROTHSTEIN**  
CHIEF OF EXTERNAL AFFAIRS

**ELIZABETH HILLIARD**  
ACTING DIRECTOR OF GOVERNMENT RELATIONS

### **POSITION ON PROPOSED LEGISLATION**

**BILL: House Bill 946 Criminal Law- Theft- Mail and Packages (Porch Privacy Act of 2024)**

**FROM: Maryland Office of the Public Defender**

**POSITION: Unfavorable**

**DATE: 02/16/2024**

The Maryland Office of the Public Defender respectfully requests that the Committee issue an unfavorable report on House Bill 0946.

House Bill 0946 makes the stealing of mail or packages a felony punishable by imprisonment not exceeding five years. While the Office of the Public Defender acknowledges and does not make light of the inconvenience, annoyance, and deprivation that a stolen package creates, the detriment to communities that will be done in making these acts a felony far outweighs the benefits.

Theft of a package is already a crime punishable by fines and incarceration, the amounts being determined by the value of the item/ items stolen. Increasing penalties does not deter crime.<sup>1</sup> The swiftness of and certainty of being caught deters crime. By making the crime of stealing mail or packages a felony, it will not prevent these crimes from happening but will only exacerbate all of the issues connected with felony convictions.

Changing the classification of crimes from misdemeanors to felonies does not prevent crime and does not improve public safety.<sup>2</sup> Creating more felonies only increases the collateral consequences of convicted people, which results in increasing the possibility of recidivism and further diminishing public safety in the communities.

Collateral consequences are legal restrictions that disqualify people convicted of crimes from accessing certain needs and benefits available to other citizens.<sup>3</sup> Many of the collateral

<sup>1</sup><https://www.ojp.gov/pdffiles1/nij/247350.pdf>

<sup>2</sup> <https://www.ojp.gov/pdffiles1/nij/247350.pdf>

<sup>3</sup> <https://niccc.nationalreentryresourcecenter.org/>

consequences experienced by people with felony convictions involve their very basic needs including employment, housing and public food benefits.<sup>4</sup> Without the possibility of stable housing and income to provide for food and other necessities, people are not safe and communities are not safe. When people do not have what they need the possibility of crime dramatically increases.

Felonies are the highest level of crime. As such, people with felony convictions face increased challenges in gaining employment. Eighty-seven percent of employers conduct background checks. Most employers do not hire people with felony convictions and/or who have served time in prison. Sixty percent of incarcerated people remain unemployed one year after their release. This inability to gain employment desperately impacts a person's quality of life and ability to establish a livelihood without committing crime.

Similarly, without employment, a person re-entering society cannot provide him or herself housing if they have no income to pay for it. At the same time, people with felony convictions are unable to access public housing and housing voucher programs. Most, if not all, government housing disqualifies applicants with felony convictions. Furthermore, families that live in public housing or have housing through a government voucher, are often not allowed to have family members with felony convictions live with them. Additionally, most landlords often do background checks and do not rent to people with criminal backgrounds and specifically felony charges. This means that a person with a felony conviction not only faces significant barriers accessing housing but is most likely unable to access affordable housing because of their conviction. They could also be prohibited from reunifying with their families if their family lives in any form of public housing.

Lastly, people with felony convictions are excluded from participating in food supplement programs in Maryland. With the prices of food on the rise, limited income and no access to food supplement programs, the options for a convicted felon to survive and meet their basic needs without reoffending are little to none.

---

<sup>4</sup> Other collateral consequences specific to Maryland are prohibitions of professional licensing, ineligibility for some civil legal assistance, prohibition from state retirement benefits, no voting rights and disqualification of jury to name a few.

Theft is often a crime of necessity or at the least a crime rooted in lack mainly lack of resources and lack of opportunity. Creating situations that further aggravate the needs of people who are already under- resourced and underserved will not decrease crime in general or the theft of mail and packages specifically but may decrease public safety by further disadvantaging already marginalized groups.

**For these reasons, the Maryland Office of the Public Defender urges this Committee to issue an unfavorable report on House Bill 0946.**

---

**Submitted by: Maryland Office of the Public Defender, Government Relations Division.**