

GA24.Testimony in Support of SB0373.MCPD.Chief Jon

Uploaded by: Captain Stacey Flynn

Position: FAV



DEPARTMENT OF POLICE

Marc Elrich
County Executive

Marcus G. Jones
Chief of Police

Statement of Chief Marcus Jones
Montgomery County Department of Police

In Support of SB 0373
The Safe Carrier Act
February 01, 2024

In the past six months, there have been multiple well-publicized local incidents of mail carriers being robbed of USPS property, including being violently robbed of their arrow keys. Investigators have discovered that arrow keys can be sold or traded for a significant profit and are a highly sought-after commodity among criminal entities.

An arrow key is one of the most powerful tools in an identity thief's arsenal. An arrow key allows a thief to open any blue US Post box, steal letters from within, and then use those stolen letters and bills to drain bank accounts, committing fraud and identity theft, most commonly against our vulnerable older populations.

While these offenses have traditionally been federal violations, Senator Waldstreicher proposes a local-level law, Senate Bill 0373, the Safe Carrier Act, that will enable Maryland law enforcement officials to charge offenders at the local level without always requiring the assistance of our Federal US Postal Service partners.

From the perspective of our Maryland victims, mail carriers, and identity theft victims, this alternate option enhances the chances of suspects being held accountable. While current police department staffing may not allow us to immediately utilize the option, having the ability to do so in the future, when department staffing levels improve, will be an excellent tool for investigators and a viable alternative option for residents and victims.

For these reasons, the Montgomery County Department of Police supports SB 0373, The Safe Carrier Act.

Chief J. Thomas Manger Public Safety Headquarters - 100 Edison Park Drive Gaithersburg, Maryland 20878
www.montgomerycountymd.gov - www.mymcpnews.com - ChiefMCPD@montgomerycountymd.gov

montgomerycountymd.gov/311



301-251-4850 TTY

SB0373 - FAV- GR24.pdf

Uploaded by: Evan Richards

Position: FAV



SB 373 – Criminal Law – Theft – Mail and Mail Depository Key

Committee: Senate Judicial Proceedings Committee

Date: February 2, 2024

Position: Favorable

The Maryland Bankers Association (MBA) **SUPPORTS** SB 373. This legislation prohibits the theft of mail and mail keys, and establishes penalties based on the severity of the theft. 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 U.S. 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. SB 373 modernizes Maryland’s theft statute and arms prosecutors with additional tools to help protect Maryland residents.

Accordingly, MBA urges issuance of a **FAVORABLE** report on SB 373.

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.



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. Mail¹ (hereinafter “mail theft-related check fraud”), the Financial Crimes Enforcement Network (FinCEN) is issuing this alert to financial institutions² 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.³ Fraud is also one of the anti-money laundering/countering the financing of terrorism (AML/CFT) National Priorities.⁴

FinCEN is issuing this alert in close collaboration with the United States Postal Inspection Service (USPIS)⁵ 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,⁶ criminals have been increasingly targeting the U.S. Mail since the COVID-19 pandemic to commit check fraud.⁷ 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.⁸ 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.⁹ 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.¹⁰

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.¹¹ 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.¹²

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.¹³

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,¹⁴ 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.¹⁵ There have also been cases of corrupt Postal Service employees who unlawfully provide Arrow Keys to criminal actors to facilitate mail theft.¹⁶ 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.¹⁷ 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.¹⁸ 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.¹⁹

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.²⁰
- 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 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.²¹ All statutorily defined financial institutions may voluntarily report suspicious transactions under the existing suspicious activity reporting safe harbor.²²

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.²³ 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.²⁴ 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).²⁵

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.²⁶

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),²⁷ Report of Cash Payments Over \$10,000 Received in a Trade or Business (Form 8300),²⁸ Report of Foreign Bank and Financial Accounts (FBAR),²⁹ Report of International Transportation of Currency or Monetary Instruments (CMIR),³⁰ Registration of Money Services Business (RMSB),³¹ and Designation of Exempt Person (DOEP).³² 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.³³ 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.

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

Final Letter Supporting SB374 2-2024.pdf

Uploaded by: Jason Shoemaker

Position: FAV



J. CHARLES SMITH, III
STATE'S ATTORNEY

KIRSTEN N. BROWN
DEPUTY STATE'S ATTORNEY

STATE'S ATTORNEY FOR FREDERICK COUNTY

County Courthouse
100 West Patrick Street
Frederick, Maryland 21701

www.statesattorney.us

CIRCUIT COURT DIVISION
301-600-1523

DISTRICT COURT DIVISION
301-600-2573

CHILD SUPPORT DIVISION
301-600-1538

JUVENILE DIVISION
301-600-2980

February 1, 2024

The Honorable William C. Smith, Jr.
Chairperson, House Judicial Proceedings Committee
2 East
Miller Senate Office Building
Annapolis, MD 21401

Dear Chair Smith and Members of the Senate Judicial Proceedings Committee:

I am Assistant State's Attorney Jason Shoemaker, and I am the Chief of the Economic Crimes Unit at the Frederick County State's Attorney's Office, who I am here on behalf of, as well as my elected State's Attorney, Charlie Smith, and the Maryland State's Attorneys' Association, in support of Senate Bill 373 – Theft – Mail and Mail Depository Key, sponsored by Senator Waldestreicher.

During my 21 years as a prosecutor, I have prosecuted a broad range of crimes, but most of my career has involved prosecuting burglary, felony theft and arson related offenses. As a local prosecutor in Frederick County, I have prosecuted, and am reviewing currently, cases where the evidence shows that mailboxes were/are targeted for the purpose of stealing mail deposited therein.

The types of harm to victims of mail theft ranges from identity theft to stolen checks. In my recent cases the check losses ranged from thousands to hundreds of thousands of dollars per stolen check.

As I was preparing my remarks in support of this bill, I located many recent articles reporting on this crime. Mail theft certainly appears to be on the rise all around the country. And it is a problem here in Maryland as well with a federal grand jury, in January, indicting five Maryland men in a fraud scheme involving the theft of over 600 checks with a face value of more than \$5 million dollars. That case included allegations of theft of checks from United States Postal Service deposit boxes.

After all, the U.S. Mail is a system which depends on and must have protected its position of reliability and trust. When you put something in the mail such as a check to pay a bill, an application with a deadline, or your tax return, you expect it to reach its destination. Likewise, if someone is trying to reach you with important information like a court date, a medical matter, or a financial notification, you should be able to rely on the U.S. Mail to get that to you.

I further note from personal and professional experience that despite the increase in conducting financial transactions digitally, the U.S. Mail remains a vital part of the American economic financial transaction process. Even when a person uses an electronic banking option, routinely, that still results in a paper check being issued on your behalf, through the mail, except now via a bank or third party processor.

It is the knowledge of the value of personal identifying information, the potential to acquire these paper checks and the potential financial windfall of this crime compared with the low likelihood of detection, apprehension, and lack of serious consequences which leads to the U.S. Mail, whether in unsecured rural mailboxes, locked community cluster or US Post Office depository mailboxes, being the targets of these thieves.

The U.S. Mail is important to all citizens and its security as a means of sending and receiving communications in the interest of all of us. Theft of any mail which is reported and prosecuted is a serious offense against the integrity of the whole system, regardless of the amount of financial loss and should be prosecuted as a felony offense.

The proposed addition of 7-106.1 to the Criminal Law Article fills a void and equips police agencies and prosecutors with a viable tool to combat this specific type of crime when it occurs in our communities. Thank you for the opportunity to provide support for this bill and I urge this Committee to issue a favorable report on Senate Bill 373.

Sincerely,

A handwritten signature in black ink, reading "Jason S. Shoemaker". The signature is written in a cursive style with a large, sweeping initial "J".

Jason S. Shoemaker,
Chief, Economic Crimes Unit

SB0373_CoA_fav.pdf

Uploaded by: Leslie Frey

Position: FAV



COMMISSION ON AGING

January 31, 2024

Judicial Proceedings Committee
Senator William C. Smith, Jr., Chair
Senator Jeff Waldstreicher, Vice Chair
2 East Miller Senate Office Building
11 Bladen Street
Annapolis, MD 21401

SUPPORT: SB 373 Criminal Law – Theft – Mail and Mail Depository Key

Dear Senator Smith:

I am writing on behalf of the Montgomery County Commission on Aging in support of SB0373. The Commission is authorized by the Older Americans Act, P.L. 116 131, and was established by Montgomery County in 1974 to advise County government on the needs, interests and issues of older adult residents, and to advocate on their behalf at the local, state and national levels.

SB0373 introduces a crucial addition to state law by creating a criminal penalty for mail theft, a provision that was previously absent. It further delineates escalating penalties based on the severity of the offense, such as the amount of mail stolen, theft from elderly or vulnerable citizens, theft of mail containing personal identifying information, and assault of mail carriers.

Montgomery County boasts a diverse and engaged older adult population, with residents 60+ constituting 22 percent of the County's total population, with a projected growth to 35 percent by 2040. Some older individuals cannot get to the post office and may rely more on the blue boxes or their own mailboxes than the rest of the population. Unfortunately, mail theft and assaults on postal carriers have become pressing concerns statewide. Instances include direct theft from blue mailboxes and armed robberies of mail carriers for their "arrow keys," a tool used to access mail receptacles in neighborhoods.

The Montgomery County Commission on Aging views the changes proposed by SB0373 as a critical step in deterring and penalizing the rising frequency of these crimes. Here are some alarming incidents that underscore the urgency of addressing this issue:

- In January 2023, a man in Silver Spring was accused of robbing a U.S. Postal carrier at gun point.¹

¹ <https://www.wusa9.com/article/news/local/maryland/man-charged-armed-robbery-mail-carrier-montgomery-county/65-d9739bb9-81f4-4007-8894-355a11610533>

Department of Health and Human Services

401 Hungerford Drive, 4th Floor, Rockville, Maryland, 20850 240-777-1120, FAX 240-777-1436

www.montgomerycountymd.gov/hhs

- In April 2023, a postal worker in Chevy Chase threatened with a gun and robbed of USPS property.²

A January 2024 AARP article cites a 2023 Gallup poll³ revealing more than twice as many Americans fear being the victim of a scam or having their identity stolen than fear being murdered. By making mail theft a state crime, including the abuse of "Personal Identifying Information," and imposing the extra sanctions on a victim who is an "elderly person" (age 68+) or a "vulnerable adult" will have special impact on older adults by reducing the stress and fear of being a victim of these crimes. Enacting SB0373 provides a swifter avenue for the State's Attorney's to pursue these egregious cases, alleviating federal resources for more complex cases.

In conclusion, the Montgomery County Commission on Aging supports SB0373, recognizing it as a vital measure to strengthen state laws against mail theft, assault of mail carriers, mail identity theft, and theft from elderly or vulnerable citizens. The Commission urges your support of SB0373, considering it a crucial step in enhancing the safety of USPS workers and vulnerable elderly residents. Tackling this escalating problem today will contribute to preserving the integrity of one of our most longstanding, dependable, and valued public services.

Sincerely,

David Engel

David Engel, Chair

Montgomery County Commission on Aging

² <https://patch.com/maryland/bethesda-chevyCHASE/usps-letter-carrier-robbed-gunpoint-chevy-chase-officials>

³ <https://news.gallup.com/poll/544643/scams-relatively-common-anxiety-inducing-americans.aspx?version=print>

Written Testimony - Louis DiRienzo (002).pdf

Uploaded by: Louis DiRienzo

Position: FAV



Statement of Lous DiRienzo Chief Counsel of the U.S. Postal Inspection Service

February 2, 2024

I am Louis DiRienzo, United States Postal Inspector, and Chief Counsel for the U.S. Postal Inspection Service. The Postal Inspection Service is the federal law enforcement and security arm of the United States Postal Service. Our agency works diligently to enforce criminal laws to protect the U.S. Postal Service (“USPS” or “Postal Service”) employees, customers, and our nation’s mailstream. I recognize that your constituents depend on the Postal Service for safe and reliable transmittal of mail, and I thank you for the opportunity to speak with you today.

Unfortunately, mail theft and robberies of USPS letter carriers have risen dramatically. Robberies of USPS letter carriers have traditionally occurred because the assailant sought to steal personal items from the carrier, such as cell phones, jewelry or cash. Over the past few years, however, we have seen a shift in criminal activity. Organized criminal groups have increasingly sought to rob USPS letter carriers for their postal keys, in order to steal U.S. Mail from receptacles and commit financial crimes. Postal keys, sometimes also called arrow keys, are keys that permit access to collection boxes, outdoor parcel lockers, cluster box units, and apartment panels in a given geographic area. The Postal Service and the Postal Inspection Service maintain accountability of postal keys to ensure they are not lost or stolen. However, this has led to robberies of carriers being a significant method criminals use to obtain keys.

Once in the hands of bad actors, criminals utilize the keys to steal large volumes of mail, which we call “volume attacks.” Criminals have always sought immediate financial gain through the theft of cash and merchandise in the mail. Criminals have also sought to steal checks in order to “wash,” or alter, the information on the check to fraudulently cash it. Often, these thefts were committed by people experiencing addiction issues for a for a quick payday and were relatively unsophisticated. However, the dark web and encrypted messaging apps have created forums that criminals exploit to sell stolen checks and personal identifying information to commit identity theft. This has shifted from the theft of mail being committed by lone actors and small informal groups to large, organized criminal elements. Stolen checks and personal identifying information are a new currency and are traded amongst criminals online with often devastating financial effects to victims.

To counter this trend, the Postal Service and the Postal Inspection Service launched the Project Safe Delivery initiative to prevent the theft of mail, to protect the mail and letter carriers, and to increase the enforcement of criminal laws. We are upgrading blue collection boxes with high security features, including electronic components. We are raising awareness through public education messaging and training our employees and law enforcement partners. And when robberies and mail theft do occur, postal inspectors enforce the laws that protect our employees and the nation's mail, collaborating with prosecutors and other law enforcement agencies at the federal, state, and local level.

The legislation before this committee would significantly enhance the ability of law enforcement to investigate robberies of letter carriers and the theft of mail in Maryland. For example, in the course of investigating a robbery, law enforcement will often catch a suspect in possession of the postal key taken from the carrier. Depending on the other evidence established, the suspect may or may not have been associated with the robbery. Unauthorized possession of a postal key is illegal federally, but under Maryland law these keys are not provided any special protection or status, even though they give criminals access to a vast amount of personal and financial information that may be contained in collection boxes, apartment panels, and other mail receptacles. This bill would fill this critical gap and give law enforcement the tools to charge those who we can only establish possessed the fruits of the robbery.

Additionally, the legislation before this committee seeks to update and modernize Maryland law to keep Marylanders' finances safe. In Maryland, basic theft charges lack the ability to effectively address the issue. Maryland grades theft by the value of the property, but mail containing PII is typically valueless for charging purposes. This bill recognizes that mail containing PII is extremely valuable to both victims and criminals and treats the theft of mail or possession of stolen mail as such.

Another critical gap that would be filled by this bill is juvenile crime. As you may be aware, there is no juvenile justice system federally. In instances in which a juvenile is apprehended in possession of stolen mail or a stolen postal key, federal prosecutors must decide whether to charge the juvenile as an adult in the federal system or let the perpetrator walk. We have observed juvenile actors being used at various levels of criminal organizations, often due to the very fact that there will be few consequences if caught. With a strong law on the books in Maryland, law enforcement and prosecutors could work collaboratively to seek justice and rehabilitation through Maryland Juvenile Services.

The legislation proposed does not replace or usurp the federal laws on mail theft, financial crimes, and assault and robbery of federal employees. Rather, it is complimentary to existing federal law and the work being done in the federal court system. As discussed above, lone actors and informal criminal groups have largely been supplanted with sophisticated organized criminal elements. While federal charges may be appropriate for some members of the groups, state charges may be most appropriate for others. As with juveniles, this law will give law enforcement and prosecutors the flexibility needed in many instances to seek justice, deterrence and rehabilitation. Further, as is the case with drug trafficking organizations, charging one member of the organization is often a

way to build a case against a group's leadership. This bill would give federal law enforcement and prosecutors the ability to work together with Maryland law enforcement and prosecutors to investigate, disrupt and dismantle entire criminal organizations through a collaborative effort at the state and federal level.

Postal inspectors are proud to work diligently alongside local Maryland law enforcement and prosecutors to protect Maryland Postal Service employees and keep Maryland postal customers' mail safe, and this bill would enhance our ability to carry out this mission. Thank you.

SB 373 Testimony R. Doyle NARFE Feb 2, 2024.pdf

Uploaded by: Robert Doyle

Position: FAV



Statement of the Maryland Federation of National Active and Retired Federal Employees

**Senate Judicial Proceedings Committee Hearing, February 2, 2024
On Senate Bill 373 – Criminal Law - Theft – Mail and Mail Depository Key**

(Position – FAV)

Good afternoon, Chair Smith and Vice-Chair Waldstreicher and members of the Judicial Proceedings Committee. My name is Robert M. Doyle and I am testifying on behalf of the State Legislative Committee of the Maryland Federation of the National Active and Retired Federal Employees Association (NARFE), representing approximately 300,000 federal annuitants and employees in Maryland. For the continuing protection and benefit of our senior membership as well as all Maryland seniors, we support – and ask you for a favorable report on – Senate Bill 373, entitled Criminal Law – Theft – Mail and Mail Depository Key.

While mail theft is prohibited by Federal law, if SB 373 becomes law, Maryland will join numerous other states which have adopted mail theft laws. This is important not only as an additional deterrent factor

but also it would allow state prosecution of someone charged with mail theft if Federal prosecution does not occur.

SB 373 addresses mail theft in Maryland in several ways. If enacted, it would make all of these actions felonies in Maryland:

- 1) theft of mail from mail boxes and mail depositories like the multiple mail boxes in apartment or condominium lobbies;
- 2) theft of Arrow Keys which US Postal Service carriers use to open mail depositories; and
- 3) theft of mail with intent to commit identity theft with special provisions when this happens to elderly persons (which HB 318 defines as someone at least 68 years old) and vulnerable adults (which MD Article – Criminal Law sec. 3-604(a)(10) defines as an adult who lacks the physical or mental capacity to provide for the adult's daily needs.)

Identity theft from seniors is a major crime. Statistics from the Federal Trade Commission for 2022 show nationally over 177 thousand reports of identity theft from consumers 60 years old and older. The

FTC statistics did not break down numbers for seniors state by state, but for Maryland as a whole, we had over 20 thousand reports of identity theft collected by the FTC in 2022.¹ Although I was unable to find any hard statistics on senior identify theft in Maryland resulting from mail theft, I can tell you that identify theft is a worrisome concern for seniors from listening to my NARFE Annapolis chapter members. Identity theft affects us all, but it can be especially harmful for seniors and vulnerable adults who often lack the financial resources to recover from identity theft. For this reason, while we endorse the entirety of SB 373, we especially appreciate how the bill offers special emphasis to elderly persons and vulnerable adults who become victims of identity theft.

This special emphasis is demonstrated in the penalties the SB 373 will impose on violators. The strongest penalties both in terms of the potential prison terms and potential fines imposed are for those charged with mail theft for the purpose of identity theft from elderly persons or vulnerable adults. This includes a minimum of 2 year incarceration for someone convicted of theft of a single item or a small number of items of

¹ Consumer Sentinel Network Data Book – 2022, Federal Trade Commission, Washington, DC, February 2023.

mail for identity theft from an elderly person or vulnerable person, and longer minimum terms when the person convicted has stolen larger quantities of mail, perhaps evidence of an ongoing scheme.

Because we support bills like this one that help seniors stay in Maryland because they feel protected here, and provide solid reasons to not retire to other states, Maryland NARFE asks respectfully for the Committee to give a favorable report to SB 373. Thank you for the opportunity to testify today.

Robert M. Doyle
Vice-Chair, State Legislative Committee
MD Federation – NARFE
4226 Carvel Lane
Edgewater, MD 21037
Bdoyle47@verizon.net
H (410) 798-0079
C/Text (301) 693-1774

SB0373 Safe Carrier Act 2024.pdf

Uploaded by: Tracy Wright

Position: FAV



People on the Go of Maryland

SB 373 (cross-filed with HB 318)

Criminal Law - Safe Carrier Act

Prohibiting the theft of mail from a mail depository owned by the United States Postal Service; prohibiting the theft of a device used to open a mail depository owned by the United States Postal Service; prohibiting the theft of mail with intent to commit identity theft; prohibiting the theft of mail from an elderly person or a vulnerable adult with intent to commit identity theft; and establishing penalties for violations of the Act.

Position: Support

Hearing February 2, 2024, 10:30 am

Sponsored by Senator Waldstreicher

Assigned to Judiciary

Written by Mat Rice

Executive Director - People On the Go of Maryland

Honorable chairperson, and distinguished members of the House Judiciary Committee:

People On the Go of Maryland (POG) is a statewide self-advocacy organization, ran for and by those with intellectual and/or developmental disabilities (IDD), and our mission is to promote self advocacy throughout the state.

POG respectfully offers this written testimony in support of Senate Bill 373 (SB 373).

This bill would increase the penalties for unlawfully accessing a mail depository, stealing a mail depository key, and stealing mail with the intent to commit identity theft against elderly persons, persons with disabilities, or other vulnerable adults.

We support this legislation because:

- Many of our members still rely on traditional postal mail to get access to the information they need, to pay their bills, and more.
- People with disabilities are more likely to be victims of identity theft, than our peers without disabilities.
- Due to forced reliance on SSI, Medicaid, and other means-tested programs, if a person with a disability has their identity stolen, they most likely will not have the financial means to track down or prosecute any individual(s) who stole their private, personal information.
- They may not even know how to do so, or where to begin to find out how.
- Many police departments lack the resources and time to pursue criminals who engage with this type of activity.
- When individuals with disabilities attempt to report such a crime, they may not even be taken seriously, due to social stigma against them.

For these reasons, we support any measure which cracks down on crimes of this type, to protect persons with disabilities and other vulnerable groups.

Therefore, we support this legislation, and respectfully ask for a favorable report on SB 373. Thank you for your consideration.

Should you have any questions please contact Mat Rice.

Thank you,

Mat Rice, Executive Director

M: 410-925-5706

E: mat@pogmd.org