## UNITED STATES DISTRICT COURT FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:
	:
	:
v.	:
	: Case No. 24-cr-545 (JMC)
	:
NIKHIL PAREKH,	:
	:
	:
Defendant.	:

#### **GOVERNMENT'S MEMORANDUM IN AID OF SENTENCING**

As part of his work for a government contractor specializing in disposing of information technology ("IT") assets, Defendant Nikhil Parekh ("Defendant") was entrusted with handling digital devices from government agencies, some of which may have contained sensitive information, and ensuring that they were safely destroyed and rendered beyond use. Yet instead of performing that valuable service for the agencies with which his employer had contracted, the defendant instead conspired with his fellow employees to steal these digital devices, sell them for their own profit, and then falsely represent to their employer that the IT equipment had been destroyed. In balancing the seriousness of his offense and the value of deterring similarly situated individuals from engaging in the same criminal conduct against defendant's early acceptance of responsibility and demonstrated remorse, the government asks the Court to sentence the defendant to a total term of 12 months' probation and to order the defendant to pay restitution. The United States of America, by and through its attorney, the United States Attorney for the District of Columbia, respectfully submits the following memorandum in support of its recommendation.

## I. PROCEDURAL BACKGROUND

On December 4, 2024, the United States filed a single-count Information charging the defendant with Conspiracy to Sell Stolen Goods, in violation of 18 U.S.C. § 371. *See* ECF No. 1. On February 4, 2025, the defendant pled guilty before this Court pursuant to a written plea agreement with the United States. *See* ECF No. 8. The Court set a sentencing date of May 5, 2025, and referred the matter to the U.S. Probation Office for the District of Columbia ("USPO") to complete a pre-sentence investigation report.

# II. FACTUAL BACKGROUND

In support of his plea of guilty, the Defendant agreed to and acknowledged the following factual proffer.

# **INTRODUCTION**

# COMPANY #1

COMPANY # 1 was an international information technology ("IT") asset disposition company headquartered in Cork, Ireland, with locations across the United States, including in the broader Washington, D.C.-metropolitan region.<sup>1</sup> More specifically, COMPANY # 1 contracted with public and private entities in the United States and abroad to securely destroy a variety of media, including hard drives, laptops, printers, tablets, smartphones, memory devices, USB sticks, CDs, and tapes. COMPANY # 1 offered both on-site and offsite destruction services, with the former involving COMPANY # 1 bringing a specialized truck to the client site and having its employees operate four shaft shredders with screens that destroyed any type of media rendering the data unrecoverable, with residual, shredded materials being recycled. Upon completion of the destruction of the relevant IT assets, COMPANY # 1 would issue a Certificate of Destruction to its customers that the relevant material had been put beyond use, completely dismantled and recycled in an environmentally responsible manner, and any data storage devices had been effective destroyed pursuant to standard data destruction processes outlined in the National Institute of Science and Technology's Guidelines for Guidelines for Media Sanitization.

# Relevant Individuals

Defendant was an employee of COMPANY # 1 from February 13, 2019 through September 15, 2023, during which time he was based out of the company's Hyattsville, Maryland location. Defendant was largely employed as a "driver," at the company, which meant that he drove the specially equipped COMPANY # 1 vans to client sites to either conduct onsite shredding of IT

<sup>&</sup>lt;sup>1</sup> In September 2024, COMPANY # 1 was acquired.

assets or to transport them to COMPANY # 1's secure shredding facility, which, initially, was located in Hyattsville, Maryland, before it was relocated to Winchester, Virginia.

Co-conspirator # 1 was an employee of COMPANY # 1 from July 8, 2019 through September 2023. Like PAREKH, Co-conspirator # 1 was based out of the company's Hyattsville, Maryland office / warehouse, and also served as a "driver" with the same responsibilities described for PAREKH above.

It was common during this period of time covering the acts described below for multiple COMPANY # 1 employees to be dispatched to a particular job site to assist with the requisition of the to-be-disposed items, loading them on to the specially equipped COMPANY # 1 van, and facilitating the secure shredding of the materials if the company had opted for on-site destruction services. PAREKH and Co-conspirator # 1 were frequently paired together and dispatched to the same client sites for the same jobs.

## Purpose of Conspiracy and Manner and Means

From on or about July 2022 through on or about August 2023, in the District of Columbia and elsewhere, Defendant and Co-conspirator # 1, along with others, known and unknown, agreed with one another to take items that they were tasked with destroying from the COMPANY # 1 trucks directly and then re-sell these items elsewhere, including across state lines in the Commonwealth of Virginia. The items taken from COMPANY # 1 trucks would include cellular telephones, tablets, laptops, and other electronic devices that COMPANY # 1's customers had contracted with the company to wipe, destroy, or otherwise render beyond use.

The conspiracy was carried out through the following manner and means, among others. First, Co-conspirator # 1 and PAREKH would be assigned to jobs at different client sites and given use of the company vans for transportation and shredding. Upon reaching the client site, Co-conspirator # 1 and PAREKH, and other known and unknown co-conspirators, would take custody of the IT assets, scan them into COMPANY # 1's system, and then begin removing digital devices slated for destruction from the various palettes they had received from the customers. Depending on the location of the site and the time at which they had finished allegedly providing the destruction services, they would then either take the company van directly to the electronics resellers and offload the items slated for destruction and sell them directly, or, they would bring the van back to the COMPANY # 1 warehouse, remove the items to be stolen from the van, and maintain custody of them until such time as they saw fit to sell them to an electronics reseller. At times, other employees at COMPANY # 1 who were dispatched to different client sites for either on-site shredding or transport of items for offsite shredding, would take possession of IT assets, and PAREKH and Co-Conspirator # 1 would come to acquire them prior to their destruction and sell them on to resellers for their personal gain.

#### **Overt** Acts

On or about January 20, 2023, COMPANY # 1 employees were dispatched to a warehouse in Linthicum Heights, Maryland, run by a contractor of a federal executive branch agency, AGENCY # 1. While there, COMPANY # 1 took custody of 10 pallets of government-furnished IT

equipment slated by AGENCY # 1 for disposition. The material included hundreds of smartphones, monitors, printers, scanners, personal computers, laptops, and other IT assets.

Beginning on or about March 2, 2023, PAREKH and Co-conspirator # 1 were assigned to an onsite shredding job for AGENCY # 2, a U.S. government entity, which maintained a warehouse for its to-be-disposed of items in Landover, Maryland. Over the course of two days, PAREKH and Co-conspirator # 1 took possession of more than 400 laptops, 1,300 smartphones, 70 servers, 20 cameras, and nearly 30 video-teleconference phones. Co-Conspirator # 1 returned to the warehouse for AGENCY # 2 in June 2023, and took custody of hundreds more IT assets.

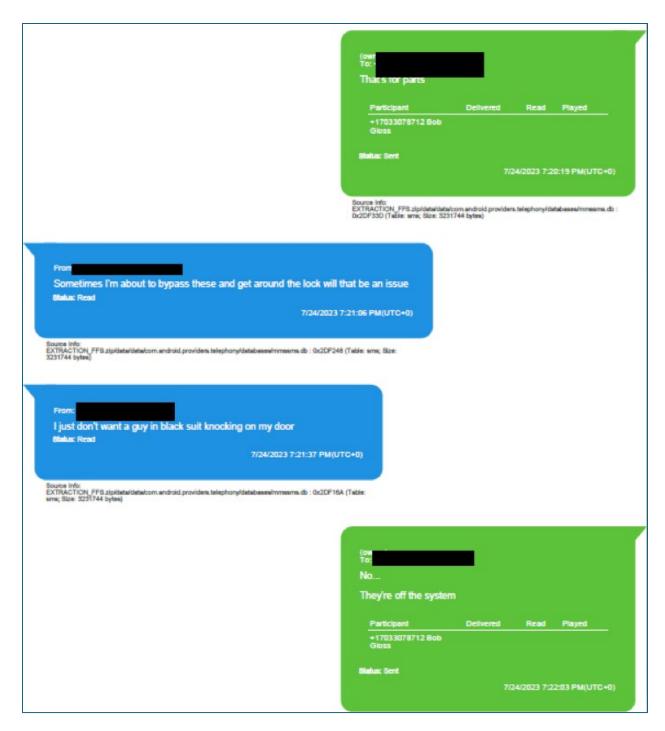
At various times during the course the conspiracy, PAREKH and Co-Conspirator # 1 were assigned to jobs at additional executive branch agencies and private businesses in Maryland, the District of Columbia, and elsewhere.

In mid-July 2023, PAREKH contacted Witness # 1, an owner of an electronics re-seller in Haymarket, Virginia, to discuss the sale of certain digital devices. Parekh ultimately dropped off numerous digital devices on July 18, 2023 at Witness # 1's electronics store, after which Witness # 1 was to conduct an inventory of the digital devices that PAREKH had dropped off and the two of them would settle upon an amount to be paid for the digital devices. During the course of the inventory, Witness # 1 noticed that many of the items that PAREKH had dropped off contained asset tag stickers on the back of them denoting to whom they belonged, including AGENCY # 2. For example.

Status: Read		
	7/24	/2023 6:50:40 PM(UTC+0)
Source Info: EXTRACTION_FFS.zip/data/ 0x2DFC38 (Table: sms; Size:	data/com.android.providers.telephony 3231744 bytes)	ridatabasesimmssms.db :
From Are these meant t	o be here?	
Status: Read Source Info: EXTRACTION: FFS.zip/data/	7/24/2023 data/com.android.providers.telephony 3231744 bytes)	7:06:45 PM(UTC+0)
0x2DFB79 (Table: sms; Size:	3231744 bytes)	
From: To: +14438013806 Ni Attachments:	khil Parekh (owner)	
To: +14438013806 N		

As demonstrated in the following excerpt, PAREKH admitted to Witness # 1 that the devices were supposed to be destroyed and that government devices were among those that were sold to Witness # 1, and at least one was connected to government cloud computing software. Out of an abundance of caution, PAREKH told Witness # 1 that the device it should be sold for parts.

From: Are these clean ? Or were they meant to be destroyed		
Slahis: Read	0.000	
7/24/2023 7:16:32	(UTC+0)	
Source Info: EXTRACTION_FF8_zipidata/databom.android.provides.telephony/databases/mmsams.db : 0x2DF700 (Table: sms; Size: 3231744 bytes)		
_		
(ow To:	iner)	
I would say 10 to 15% are clean		
All	for meant to be destroyed	
	Participant Delivered Read Played	
84	ha: Sert	
	7/24/2023 7:17:14 PM(UTC+0)	
Source EXTRU	ACTION: FFS.zip/deta/deta/com.android.providers.telephony/databases/mmsams.db : 0x2DF630 (Table: sms:	
Size: 3	2231744 Eytes)	
From: So the government isn't going to come looking for me or something Blakus: Read 7/24/2023 7:17:49 PM(UTC+0)		
Source Info: EXTRACTION_FF8_zipidata/databorn.android.providers.telephony/databases/mmsams.db : 0x2DF54A (Table: sms; Size: 3231744 bytes)		
From: - ?? Status: Read 7/24/2023 7:18:27 PM(UTC+0	η	
Source Info: EXTRACTION_FF8.zipideta/deta/com.android_providers.telephonyldatabases/mmsama.db : 0x2DF4A3 (Table: sms; 8ize: 3231744 bytes)		
	(owner) To: +	
Only the one in the cloud is going to be a problem		
	Participant Delivered Read Played +17033078712 Bob Gloss	
	Sinhu: Sert	
	7/24/2023 7:19:31 PM(UTC+0)	
	Source info:	



On July 28, 2023, PAREKH called Co-Conspirator # 1 and said that as soon as Witness # 1 paid PAREKH the money, he would send it to Co-Conspirator # 1. On August 1, 2023, Co-Conspirator # 1 and PAREKH had an additional phone call, in which PAREKH confirmed that Witness # 1 had paid him, and that he would pay Co-Conspirator # 1 in turn. The two also discussed how Co-Conspirator # 1 had recently come into possession of hundreds of iPhones and approximately two dozen tablets, and the two discussed what prices Co-Conspirator # 1 should demand upon approaching a separate electronics re-seller located in Maryland. On August 1, 2023, Witness # 1 ultimately paid PAREKH one installment for the digital devices he dropped off on

July 18, 2023, in the amount of \$1,000 through the payments application Zelle. PAREKH then immediately paid \$300 to Co-Conspirator # 1.

On August 2, 2023, law enforcement agents inspected Witness # 1's business and interviewed Witness # 1 and discovered 258 electronic items, including those of AGENCY # 1 and AGENCY # 2, all of which were identified as being part of deliveries from PAREKH, and seized them. AGENCY # 2 had confirmed it owned and turned over to COMPANY # 1 for destruction seventy-two of the electronic devices seized from Witness # 1's business. AGENCY # 2's devices were identified by red, white, and black asset tag stickers bearing a barcode, a six-digit number, and the name of AGENCY # 2. AGENCY # 1 owned and turned over to COMPANY # 1 for destruction eighteen of the electronic devices seized from Experimax. AGENCY # 2's devices were identified by black and white asset tag stickers bearing a barcode, a six-digit number, and the name of the agency. The remainder of the devices were eventually traced back to additional government agencies and private entities, which in turn confirmed that they had provided them to COMPANY # 1 pursuant to a contract under which COMPANY # 1 was to destroy them or render them beyond use and certify the same prior to payment.

PAREKH admits for the purpose of this plea agreement that he knowingly agreed with one or more other persons, including Co-Conspirator # 1, to take items provided to COMPANY # 1 for purposes of destruction, that such items would have a value in excess of \$5,000, that PAREKH and other co-conspirators would transport them across state lines, and sell them, despite knowing that the goods were to be destroyed pursuant to their responsibilities for their employer and their employer's contractual obligations for their client. PAREKH further admits that, in furtherance of this conspiracy, he and his co-conspirators did, in fact, take items—that had been given by AGENCY # 1 and AGENCY # 2 to COMPANY # 1 to be destroyed—with a value of at least \$10,000, and PAREKH and his co-conspirators did transport these items across state lines for resale for their own personal profit.

ECF No. 9. As set forth in the Statement of Offense, the foregoing facts to which the defendant

has admitted did not and do not purport to include all of his illegal conduct or a comprehensive

statement about what he knew or what he witnessed with respect to his co-conspirators' activities.

Rather, it is merely intended to demonstrate that there is a sufficient factual basis in support of the

defendant's guilty plea.

# **III.** DISCUSSION AND APPLICATION OF U.S. SENTENCING GUIDELINES AND 3553(a) FACTORS

## A. <u>Generally Applicable Legal Principles</u>

When determining the appropriate sentence, the district court should consider all of the

applicable factors set forth in 18 U.S.C. § 3553(a). See United States v. Gall, 128 S. Ct. 586, 596

(2007). The listed factors in 18 U.S.C. § 3553(a) include the following:

(1) the nature and circumstances of the offense and the history and characteristics of the defendant;

(2) the need for the sentence imposed –

(A) to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense;

(B) to afford adequate deterrence to criminal conduct;

(C) to protect the public from further crimes of the defendant; and

(D) to provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner;

(3) the kinds of sentences available;

(4) the kinds of sentence and the sentencing range established for -

(A) the applicable category of offense committed by the applicable category of defendant as set forth in the guidelines –

(i) issued by the Sentencing Commission ...; and

(ii) that, . . . are in effect on the date the defendant is sentenced; ...

(5) any pertinent policy statement –

(A) issued by the Sentencing Commission ... and

(B) that, . . . is in effect on the date the defendant is sentenced.

(6) the need to avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct; and

(7) the need to provide restitution to any victims of the offense.

## B. <u>Guidelines Calculations</u>

Turning to 3553(a)(4)(A), for the reasons set forth in its response to the Pre-Sentence Investigation Report (hereinafter, "PSR"),<sup>2</sup> the government agrees with the calculations of U.S. Probation regarding the defendant's Total Offense Level under the U.S. Sentencing Guidelines (hereinafter, "Guidelines") as well as his criminal history category.

## 1. Offense Level Calculation

The base offense level for the offense of Conspiracy to Sell Stolen Goods in violation of 18 U.S.C. § 371, is USSG §2X1.1, which provides that the base offense level is the guideline for the substantive offense, which in this case is §2B1.1. PSR at ¶ 40. 2B1.1., in turn, sets forth a base offense level of 6. Because the defendant is accountable for a total loss amount of \$10,000, two levels are added under §2B1.1(b)(1)(B). *Id.* at ¶ 41. Given that the defendant's offense involved receiving stolen property and that the defendant was in the business of selling it, an additional two levels are added under §2B1.4(b)(4). *Id.* at ¶ 42. Because the defendant meets the criteria set forth in §4C1.1 for a "Zero-Point Offender," his offense level is reduced by two levels. *Id.* at ¶ 48. Furthermore, in light of his early guilty plea pursuant to an information, he has clearly demonstrated acceptance of responsibility, entitling him to an additional two-level decrease. *Id.* at ¶ 49. Consequently, his total offense level is 6.

<sup>&</sup>lt;sup>2</sup> References to the PSR or Presentence Report are to the initial PSR and not the final one, which is not yet available. See ECF No. 69.

## 2. Criminal History

The government agrees that the defendant has no criminal convictions that can be scored for purposes of Chapter Four of the Guidelines. With zero criminal history points, the defendant is in Criminal History Category ("CHC") I.

#### *3.* USSG Range

In CHC 1, with a Total Offense Level of 6, the defendant's Guidelines range is zero to six months, in Zone A. In Zone A, a sentence of probation is authorized by the Guidelines, as are sentences of community confinement, home detention, and intermittent confinement. *See* USSG § 5B1.1, Application Note 1(A).

#### C. <u>Recommendation</u>

After calculating the applicable Guidelines range, the Court should next consider all of the applicable factors set forth in 18 U.S.C. § 3553(a), noted *supra* at III.A. Indeed, the Guidelines themselves are designed to calculate sentences in a way that implements the considerations relevant to sentencing as articulated in Section 3553(a). *Rita v. United States*, 127 S. Ct. 2456, 2463 (2007). The Court must impose a sentence that is sufficient but not greater than necessary to reflect the seriousness of the offense, to promote respect for the law, to provide just punishment, to afford adequate deterrence, to protect the public from further crimes of the defendant, and to provide the defendant with needed educational or vocational treatment. 18 U.S.C. § 3553(a)(2). The United States recommends that the Court sentence the defendant to a term of probation of 12 months, which, as detailed below, will best effectuate the purposes of sentencing as outlined in § 3553(a).

#### 1. Nature and Seriousness of the Offense

The defendant was a key player in a years' long scheme to steal devices that government agencies and private companies had entrusted his employer to wipe and destroy, sell them for the profit of the co-conspirators, and then cause the company to invoice the victim organizations for services that were never actually provided. While under the plea agreement the defendant is being held accountable for total losses of 10,000 – and has agreed to pay restitution up to the same amount to the identifiable victims of his scheme – based on how the conspiracy operated, there is ample basis to believe there are greater losses and even more victims. Indeed, when first interviewed by law enforcement in June 2024, defendant had difficult recalling precisely how many thousands of devices he had personally taken during his time with the aforementioned government contractor with which he was employed. Furthermore, the United States was only able to calculate restitution and loss amounts based on those stolen devices law enforcement actually successfully intercepted at different electronics resellers during the late summer and fall of 2023 prior to their re-sale, which was still over 500 devices. This figure, though, was, and remains, a mere snapshot in time of what stolen devices were then in circulation at the re-sellers and that law enforcement agents could actually seize. Yet, as defendant himself admitted multiple times when interviewed by law enforcement, he and others had been engaged in this scheme by mid-2022 and indeed there are multiple receipts from resellers reflecting items that he and his coconspirators dropped off during the period of the conspiracy that were almost certainly stolen. Nevertheless, such items had long since been pawned off by the re-sellers and could no longer be tracked and identified by law enforcement agents.

Furthermore, not only did defendant's scheme essentially defraud various organizations by having them pay for the destruction and recycling of devices that defendant and his co-conspirators never destroyed, but they also exposed potentially sensitive data from different government agencies by simply re-selling these devices directly on to electronics re-sellers. Indeed, as the text messages with an electronics reseller noted above demonstrate, little care was taken by the defendant to ensure there was no sensitive data on these devices prior to selling them on to second-hand stores and pawnshops. As the defendant made clear in that conversation, only "10-15 %" were "clean," that is, either still in the box or essentially unused, <sup>3</sup> while at least one device, a phone, was connected to a cloud-based system. The defendant then advised that device should be used for parts, but at that point he had already sold the device and was in no position to guard against the potential improper access of data. If anything, defendant's text messages reveal a casual disregard of any security and / or privacy risks posed by his selling to-be-destroyed devices to resellers for eventual sale to any end-user.

Overall, Defendant's conspiracy to transport and sell these stolen items resulted in significant losses to victim agencies, only a fraction of which can adequately be captured after the fact given the nature of the scheme, and resulted in the potential exposure of sensitive data from government and corporate clients of his former employer. The nature and breadth of his scheme would ordinarily warrant a significant punishment.

## 2. History and Characteristics

The PSR does not suggest that the defendant was mentally and/or emotionally incapable of avoiding his criminal conduct; instead, he chose to engage in criminal conduct intentionally and repeatedly because it was profitable. Indeed, even after the government contractor fired him from his position upon discovering the scheme, he simply went to a similar "e-waste" company where

<sup>&</sup>lt;sup>3</sup> Through its investigation, the government has learned that numerous agencies would purchase particular models of digital devices, such as phones and tablets, only for those purchases to soon become out-of-date and unusable because technological advances in operating systems had quickly rendered them less secure. As such, the agencies would dispose of these devices through the defendant's company without actually having distributed them to their employees.

he essentially engaged in the same conduct that had just resulted in his termination. Indeed, upon executing a residential search warrant on the defendant's residence in Maryland in June 2024, agents identified multiple devices that law enforcement confirmed had belonged to various organizations that had contracted with defendant's then employer to wipe and recycle, but had nevertheless been misappropriated by the defendant. In other words, termination and the end of gainful employment did little to deter the defendant in his efforts to exploit gaps in the internal controls of his employers and misappropriate items to sell for his own account.

Ultimately, the defendant is 37 years' old, has some high school education, a commercial driver's license, and a history of employment, while not suffering any emotional or physical condition, substance abuse included, that might otherwise explain his conduct during the time of the conspiracy. Rather, the defendant simply identified an opportunity for another stream of income, one that would come at the expense his employers as well as the organizations that contracted with his employers for the secure destruction of their IT assets.

#### *3. Need of the Sentence Imposed*

The government believes that its proposed sentence of 12 months' probation will best effectuate the purposes of sentencing as set forth in 3553(a)(2)(A)-(D), that is, for the sentence imposed to reflect the seriousness of the offense, promote respect for the law, and provide just punishment for the offense; afford adequate deterrence of criminal conduct; protect the public from further crimes of the defendant; and allow the defendant with training, treatment, and other type of care he may require. As noted above, the defendant's scheme – across multiple years and entailing multiple victims – is a serious one, in terms of both the financial ramifications for the victim organizations as well the implications for their data privacy and security. As important is the Court's consideration of the possible deterrent effect that a sentence in this matter may have

on others contemplating committing this type of fraudulent scheme. Section 3553(a) is not limited to the necessary sentence to deter the defendant from engaging in further criminal conduct (specific deterrence), but also includes consideration of deterring other potential criminals from engaging in similar conduct (general deterrence). See, e.g., United States v. Phinazee, 515 F.3d 511, 515-16 (6th Cir. 2008) ("The plain language of the statute . . . also militates against limiting the authority of the court to specific deterrence. . . . We note that this conclusion comports with the longstanding and uncontroversial practice of considering general deterrence in sentencing."). While ordinarily that may counsel in favor of a carceral sentence given that the misconduct at issue here was alleged by the defendant to have been pervasive and easily accomplished, necessitating a sentence that would send a strong message, there are mitigating factors unique to the defendant that government believes the Court should take into account. First, the defendant was cooperative with law enforcement from the outset, providing a lengthy interview during the execution of the search warrant for his residence. Second, the defendant agreed to plead guilty to a felony offense via an information and waived his right to be charged via an indictment returned by a duly constituted grand jury. While the Guidelines calculations already capture his acceptance of responsibility and reflect a two-level reduction with respect to his offense level, even that does not capture how early the defendant was prepared to admit his wrongdoing and make amends in the form of paying restitution. Furthermore, notwithstanding his involvement in the conspiracy and his conduct after his termination, the defendant does not have a criminal history and thus this current charge represents his first interaction with the criminal justice system. The government hopes that after this experience, including having his home searched, being charged with a federal crime, and pleading guilty, that it will be his last. Based on the foregoing, the government believes a probationary sentence of 12 months is sufficient to accomplish that goal.

#### D. The Defendant Should Be Required to Pay Restitution to the Victim

The defendant has agreed via his plea agreement with the United States to pay restitution, in an amount not to exceed \$10,000. The government is currently in the process of identifying all victim organizations, determining whether they wish for restitution in kind (i.e., the return of the devices that were never actually destroyed) or financial compensation. The government will endeavor to have a comprehensive list of victims and amounts owed to each victim by the date of the defendant's sentencing hearing.

## E. The Defendant Should be Required to Pay a Forfeiture Money Judgment

"Criminal forfeiture is not an independent substantive offense, nor is it even an element of an offense. It is instead 'an aspect of punishment imposed following conviction of a substantive criminal offense." *United States v. Day*, 416 F. Supp. 2d 79, 84 (D.D.C. 2006) (quoting *Libretti v. United States*, 516 U.S. 29, 39 (U.S. 1995)), aff'd in part on other grounds and rev'd in part on other grounds, 524 F.3d 1361 (D.C. Cir. 2008). Criminal forfeiture may take the form of: (1) an *in personam* money judgment against the defendant; (2) forfeiture of specific assets; and (3) forfeiture of "substitute assets" if the directly forfeitable assets are unavailable. *United States v. Zorrilla-Echevarria*, 671 F.3d 1, 5-6 (1st Cir. 2011) (citation omitted). Federal Rule of Criminal Procedure 32.2 governs criminal forfeitures. Here, the government requests that the Court impose an order requiring the defendant to forfeit the specific items identified in the plea agreement. The government will be submitting a proposed order of forfeiture in a future filing prior to the defendant's sentencing date.

## **IV. CONCLUSION**

WHEREFORE, for the foregoing reasons, the Court should sentence the defendant to a term of probation of 12 months, and order the defendant to pay restitution in an amount to be

determined to the identified victims of his offenses. Such a sentence would be sufficient but not

greater than necessary to achieve the purposes of sentencing.

Respectfully submitted,

EDWARD R. MARTIN, JR. United States Attorney

By: /s/ Will Hart\_\_\_\_\_ WILL HART Assistant United States Attorneys D.C. Bar No. 1029325 601 D. St., N.W. Washington, D.C. 20530 (202) 252-7877 William.hart@usdoj.gov