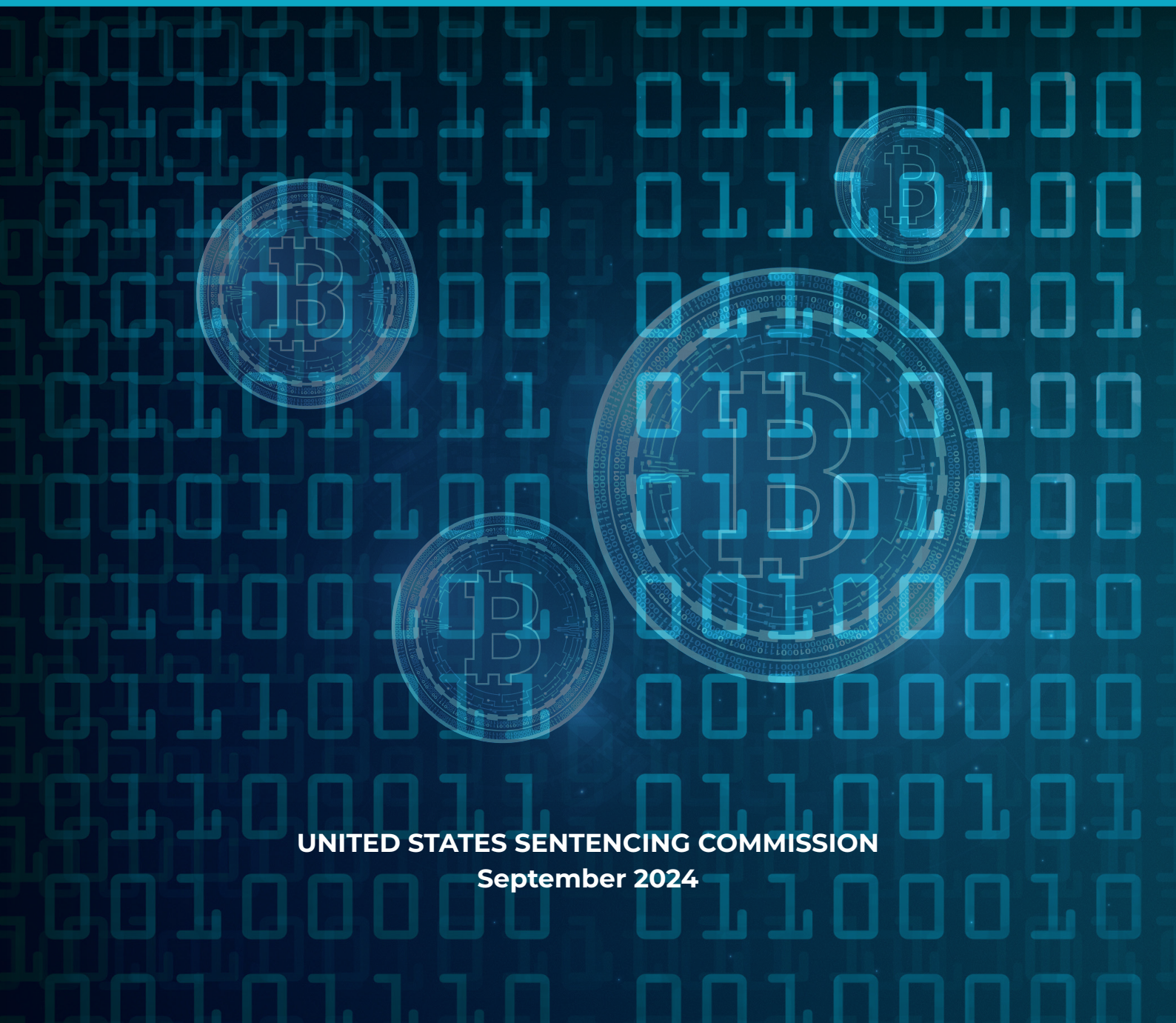
CYBER TECHNOLOGY

IN FEDERAL CRIME



UNITED STATES SENTENCING COMMISSION

September 2024

Cyber Technology in Federal Crime

CARLTON W. REEVES
Chair

LUIS FELIPE RESTREPO
Vice Chair

LAURA E. MATE
Vice Chair

CLAIRE MURRAY
Vice Chair

CLARIA HORN BOOM
Commissioner

JOHN GLEESON
Commissioner

CANDICE C. WONG
Commissioner

PATRICIA K. CUSHWA
Ex Officio

SCOTT A.C. MEISLER
Ex Officio

KENNETH P. COHEN
Staff Director

GLENN R. SCHMITT
Director, Office of Research and Data

September 2024

Table of Contents

There has been little analysis on the individuals sentenced for a federal offense who use cyber technologies for illegal purposes.

This report provides information on individuals sentenced for offenses using cryptocurrency, the dark web, and hacking for fiscal years 2014 through 2021.

Introduction

The use of cyber technologies, such as cryptocurrency and the dark web, provides new and evolving means to commit crimes and avoid detection. These technologies are used to commit a variety of federal offenses. The dark web is sometimes used to create, hide, or access websites containing child pornography. Illegal drugs and firearms are sometimes sold through dark websites.[1] Cryptocurrency is sometimes used to facilitate these crimes. As noted by the Attorney General's Cyber Digital Task Force in 2020, individuals—

> may exploit cryptocurrency to: (1) engage in financial transactions associated with the commission of crimes, such as buying and selling drugs or weapons on the dark web, leasing servers to commit cybercrimes, or soliciting funds to support terrorist activity; (2) engage in money laundering or shield otherwise legitimate activity from tax, reporting, or other legal requirements; or (3) commit crimes directly implicating the cryptocurrency marketplace itself, such as stealing cryptocurrency from exchanges through hacking or using the promise of cryptocurrency to defraud unwitting investors.[2]

Regardless of the type of crime involved, the relative anonymity these technologies provide to their users creates challenges for the investigation and prosecution of the crimes committed with them.[3]

The use of cyber technology to commit crimes transcends national borders. As Interpol has found, this causes investigative and legal challenges that can be difficult to overcome.[4] United States government agencies, such as the Federal Bureau of Investigation and the Financial Crimes Enforcement Network, have reported on the increasing threats from these technologies and estimated yearly losses in the billions from the crimes committed with these technologies.[5]

There has been little analysis on the individuals sentenced for a federal offense who use these technologies for illegal purposes, the offenses they committed, and trends in these areas over time. In developing this report, the United States Sentencing Commission ("the Commission") collected information on individuals sentenced for offenses using cryptocurrency, the dark web, and hacking for fiscal years 2014 through 2021.[6]

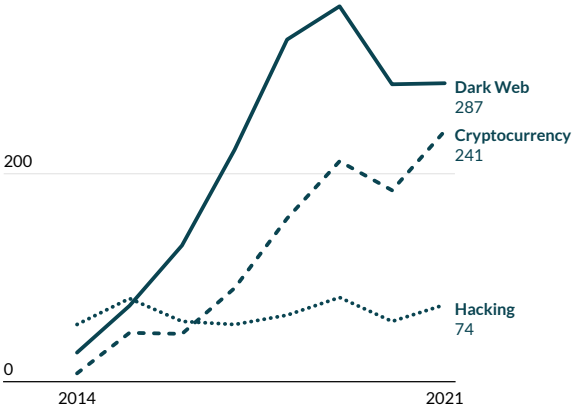
This report provides demographic and sentencing information for those individuals who used three types of cyber technology during their offenses—hacking, cryptocurrency, and the dark web—along with the types of offenses committed using these technologies. The Commission analyzed this data to draw comparisons with all other federally sentenced individuals between fiscal years 2014 and 2021 who did not use these technologies.

AUTHOR

Tracey Kyckelhahn, Ph.D.
Senior Research Associate
Office of Research and Data

Key Findings

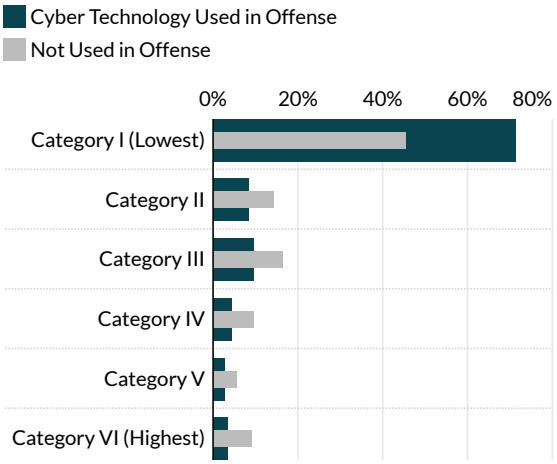
1 Between 2014 and 2021, 2,590 sentenced individuals used at least one of three types of cyber technology—hacking, cryptocurrency, and the dark web—in connection with a federal offense, and the number increased substantially during the time studied from 2014 to 2021. However, this number represented less than one percent of the total federal caseload.



2 Individuals who used cyber technology in their offense were more likely to be White, male, younger, and have completed at least some college than other sentenced individuals.

- Over two-thirds (68.6%) of individuals who used cyber technology in their offense were White, compared to 21.5 percent of other sentenced individuals.
- While 94.0 percent of those who used cyber technology were male, 86.8 percent of other sentenced individuals were male.
- Almost a quarter (22.4%) of individuals who used cyber technology had a college degree, compared to 5.8 percent of other sentenced individuals.

3 Individuals who used hacking, cryptocurrency, or the dark web in their offense had less criminal history than individuals who did not use cyber technology in the commission of a federal crime. Less than half of other sentenced individuals were in Criminal History Category (CHC) I, the lowest category.



4 The most common offenses committed by individuals who used cyber technology in their offense were child pornography (28.9%), fraud (27.5%), drug trafficking (20.6%), and money laundering (8.9%).

Crime Type	Percent
Child Pornography	28.9%
Fraud/Theft	27.5%
Drug Trafficking	20.6%
Money Laundering	8.9%
Sexual Abuse	7.0%
Firearms	1.5%
Stalking/Harassing	1.2%
National Defense	0.9%
Forgery/Counterfeit/Copyright	0.8%
Extortion/Racketeering	0.6%
Other	2.1%

Data Collection and Methodology

Identifying Cyber Technology Cases

In this report, the Commission combines data it regularly collects with data from a special coding project to provide a deeper understanding of individuals who use cyber technology in federal offenses. As a supplement to its research activities, the Commission undertook a special data collection project to identify individuals who used cyber technology in their offense. The Commission used computer technology to search Presentence Investigation Reports (PSRs), plea agreements, and indictments for individuals sentenced between 2014 and 2021 for terms identified as indicating the use of cyber technology in connection with the offense.[7] Staff then reviewed each case identified to determine if any of the three types of cyber technology were used in the offense: hacking, cryptocurrency, and the dark web. If at least one type of cyber technology was used, the type of cyber technology used by the individual was coded. This data was then combined with the data available in the Commission's regularly-collected fiscal year files to create the dataset used for the analyses in this report.

For this report, "**hacking**" includes both the creation or use of computer code in addition to phishing schemes and brute force attacks.[8] Therefore, both sophisticated hacks involving programming and lower tech hacks are included.

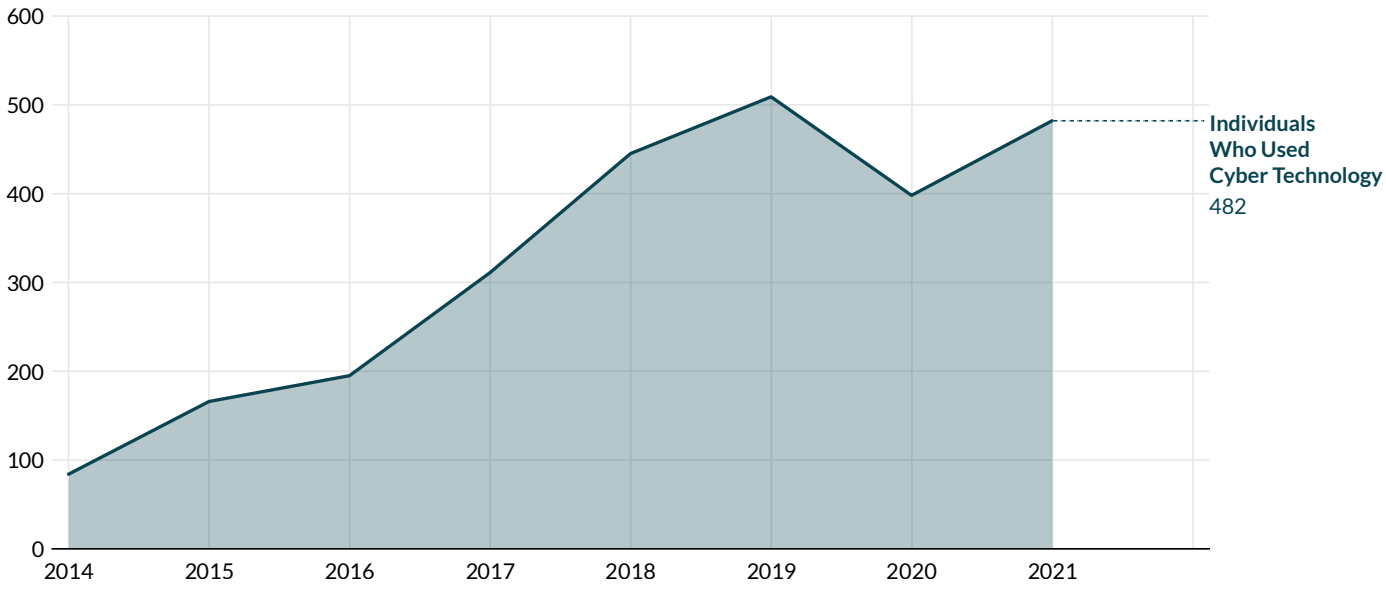
"**Cryptocurrency**" is the broad name for digital currencies that use blockchain technology[9] to work on a peer-to-peer basis.[10] Cryptocurrencies do not need a bank to carry out transactions between individuals. The cryptocurrency network keeps track of all the transactions and ensures that no one reneges on a transaction.[11] It affords greater anonymity than many other forms of payment.[12]

The "**dark web**" refers to a part of the internet located beyond the reach of traditional internet browsers.[13] It is accessible only through the use of special software and is designed to allow users and website operators to remain anonymous and difficult to trace.

In this report, the Commission provides information about all persons using cyber technology in connection with a federal offense. It does not include cases in which cyber technology was used in the offense, but not by the sentenced individual. Therefore, it is not intended to provide information on all individuals whose crimes were enabled by this technology.

Use of Cyber Technology in Federal Offenses

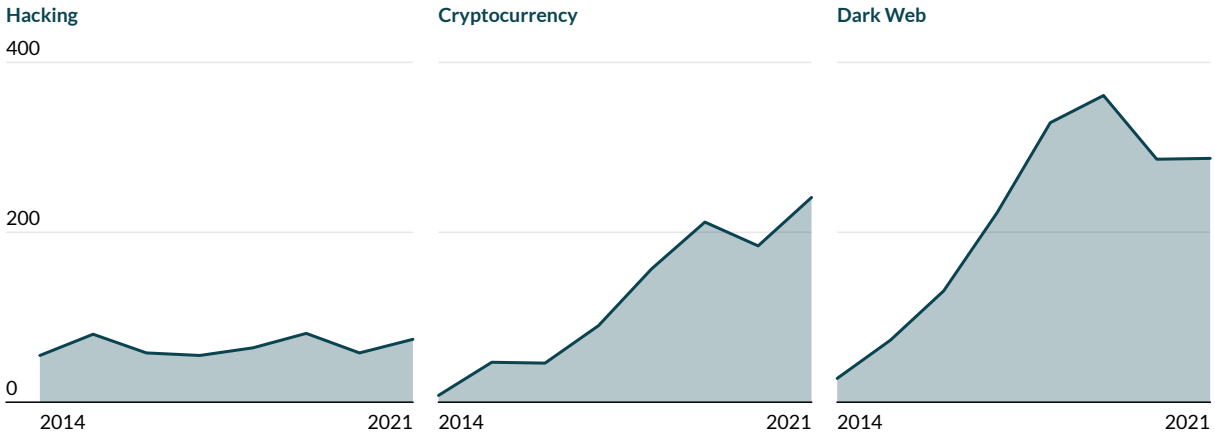
Figure 1. Cyber Technology Used by Individuals in Federal Crimes, Trends, Fiscal Years 2014–2021



This report provides information about the demographics of individuals using this technology, the crimes[14] they committed using this technology, and the manner in which courts sentenced them for their offenses. This report then examines three types of cyber technology used in these offenses and provides further analyses of the persons using each technology and the offenses committed with it. Finally, this report examines the four crime types most commonly committed by individuals who used these techniques in the commission of their offense.

Between fiscal years 2014 and 2021, 2,590 sentenced individuals used hacking, cryptocurrency, or the dark web in the commission of their federal offense. The number of individuals who used these cyber technologies or techniques increased substantially from 84 in 2014 to 509 in fiscal year 2019. In fiscal year 2020, the first year the federal caseload was impacted by the COVID-19 pandemic, 398 individuals used these technologies (0.6% of all persons sentenced federally that year) while 482 individuals used them in fiscal year 2021 (0.9% all persons sentenced federally that year).

Figure 2. Type of Cyber Technology Used by Individuals in Federal Crimes, Trends, Fiscal Years 2014–2021



Type of Cyber Technology Used

The dark web was the most common cyber technology used by individuals sentenced between fiscal years 2014 and 2021. A total of 1,718 (66.3%) of the 2,590 individuals who exploited cyber technology used the dark web in the commission of their offense. Cryptocurrency was used by 985 (38.0%) individuals, while 525 (20.3%) individuals used hacking techniques.

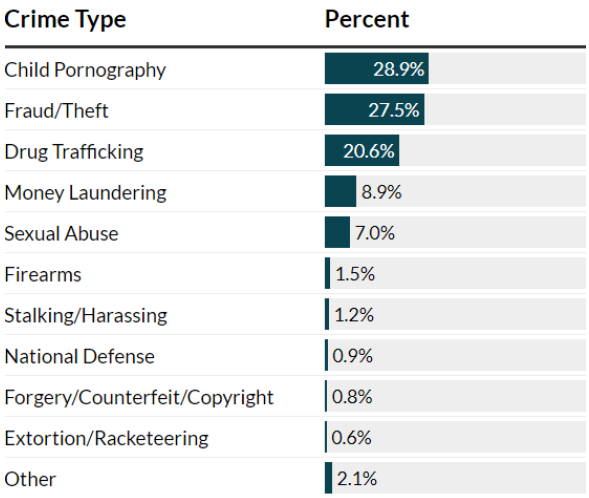
Most sentenced individuals used a single type of cyber technology. The dark web was the sole cyber technology used by 43.9 percent of individuals. Hacking was used as the sole cyber technology by 17.0 percent of individuals, and cryptocurrency alone was used by 14.9 percent of individuals.

Some individuals used multiple types of cyber technology in the commission of their federal offense. Most notably, cryptocurrency and the dark web were used together by 20.9 percent of those who used cyber technology. Hacking and cryptocurrency were used together by 1.8 percent of these individuals, followed by hacking and the dark web (1.0%). Only 0.5 percent of individuals who exploited cyber technology used all three technologies in the commission of their federal offense.

Figure 3. Type of Cyber Technology Used in Federal Offense, Fiscal Years 2014–2021

Type Used	Percent
Dark Web	43.9%
Cryptocurrency and Dark Web	20.9%
Hacking	17.0%
Cryptocurrency	14.9%
Hacking and Cryptocurrency	1.8%
Hacking and Dark Web	1.0%
Hacking, Cryptocurrency, and Dark Web	0.5%

Figure 4. Crimes Committed with Cyber Technology Assistance, Fiscal Years 2014–2021[15]



Type of Crime

The crime types of persons who used cyber technology differed considerably from that of other sentenced individuals. As shown in Figure 4, more than one-quarter of individuals who used cyber technology in their offense were sentenced for child pornography (28.9%) or fraud (27.5%), followed by drug trafficking (20.6%), money laundering (8.9%), and sexual abuse (7.0%). In contrast, one-third (33.1%) of all other sentenced individuals were sentenced for immigration, followed by drug trafficking (28.1%), firearms (10.4%), fraud/theft/ embezzlement (10.0%), and robbery (2.4%).

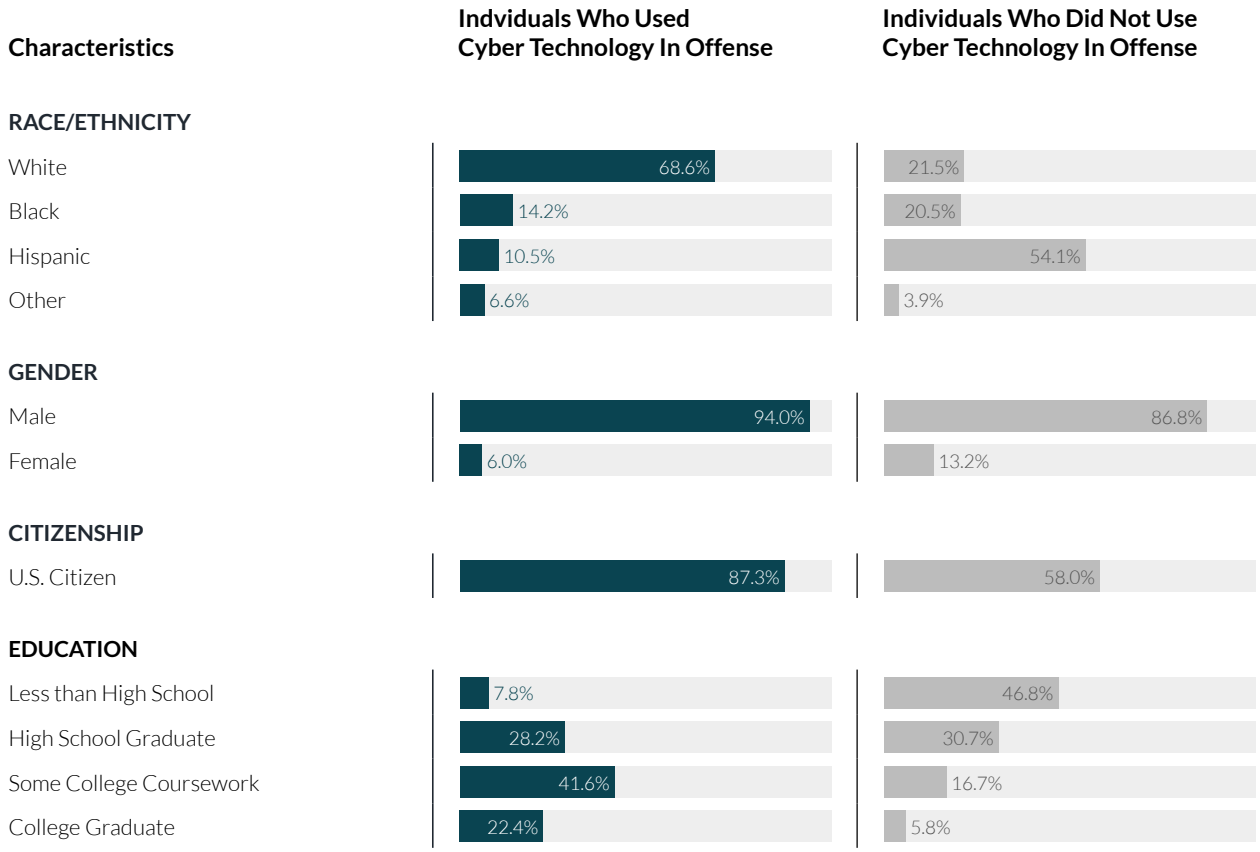
Individual Characteristics

The demographic characteristics of persons who used cyber technology differed from other sentenced individuals. Those who used cyber technology in the commission of their offense were over three times as likely to be White (68.6%) as other individuals (21.5%). Fewer individuals who used cyber technology were Black (14.2%) or Hispanic (10.5%), as compared to other sentenced individuals (20.5% and 54.1%, respectively).

Those who used cyber technology in the commission of their offense were more likely to be male (94.0%) than others sentenced (86.8%). They were also substantially more likely to be U.S. citizens than other sentenced individuals (87.3% compared to 58.0%).

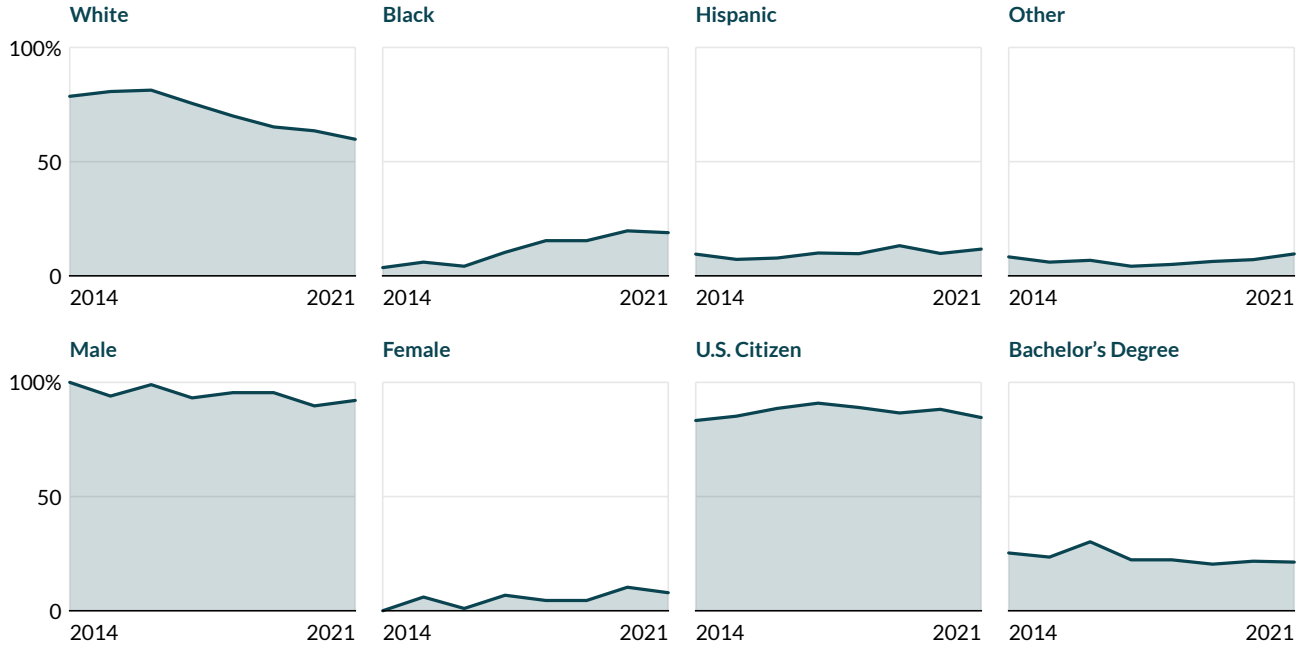
Persons who used cyber technology in the commission of an offense also had higher levels of educational attainment compared to the other sentenced individuals. The proportion of such individuals with college degrees (22.4%) was nearly four times that of other sentenced individuals (5.8%). Conversely, individuals who used cyber technology were substantially less likely to not have a high school degree (7.8%) than other sentenced individuals (46.8%).

Figure 5. Characteristics of Individuals Who Used Cyber Technology in Federal Offense, Fiscal Years 2014–2021



The proportion of sentenced individuals with college degrees who used cyber technology in their crimes was nearly four times that of other sentenced individuals.

Figure 6. Characteristics of Individuals Who Used Cyber Technology in Federal Offense, Trends, Fiscal Years 2014–2021



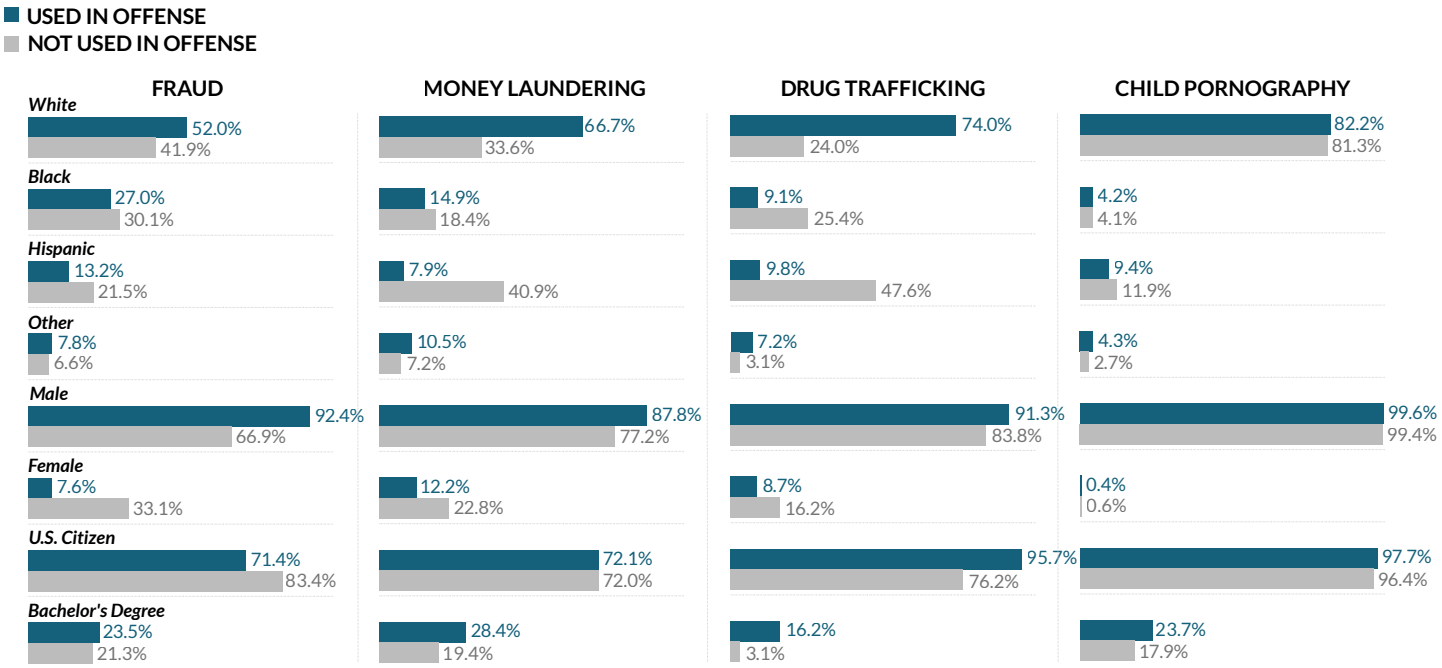
Characteristics of Individuals Who Used Cyber Technology in Federal Offenses by Type of Crime

Trends in Individual Characteristics

Some demographic characteristics of those who used cyber technology in their offense changed between fiscal years 2014 through 2021 while others were unchanged. The racial composition and median age at sentencing changed noticeably over the eight fiscal years studied. The share of White individuals who used cyber technology in their offense declined from approximately 80 percent during the first three years to approximately 60 percent in fiscal year 2021. The share of Black individuals who used cyber technology in their federal crimes increased from four percent in fiscal year 2014 to almost 20 percent in fiscal year 2021. Conversely, the proportion of White and Black individuals among other sentenced individuals remained relatively constant during this time-period, varying between 19.0 percent and 23.5 percent for White sentenced individuals and 19.1 percent and 23.1 percent for Black sentenced individuals. The median age of individuals who used cyber technology in their offense increased from 30 years in fiscal year 2014 to 34 years in fiscal year 2021. The median age of other sentenced individuals was 35 years each year from fiscal years 2014 through 2021.

Males consistently comprised approximately 90 percent or more of those who used cyber technology in their offense from fiscal years 2014 through 2021. Similarly, U.S. citizens have comprised over 80 percent of those who used cyber technology each year, and 20 percent or more of these individuals have bachelor's degrees each year.

Figure 7. Characteristics of Individuals Who Used Cyber Technology in Federal Offense by Type of Crime, Fiscal Years 2014–2021



Individual Characteristics by Type of Crime

The demographics of individuals sentenced in the federal system differed by the type of crime committed; therefore, it is useful to compare those who used cyber technology to other federally sentenced individuals who committed the same offenses. Focusing on the four most common offenses involving cyber technology, there were notable differences between the individuals who used those technologies in their offense compared to other sentenced individuals.

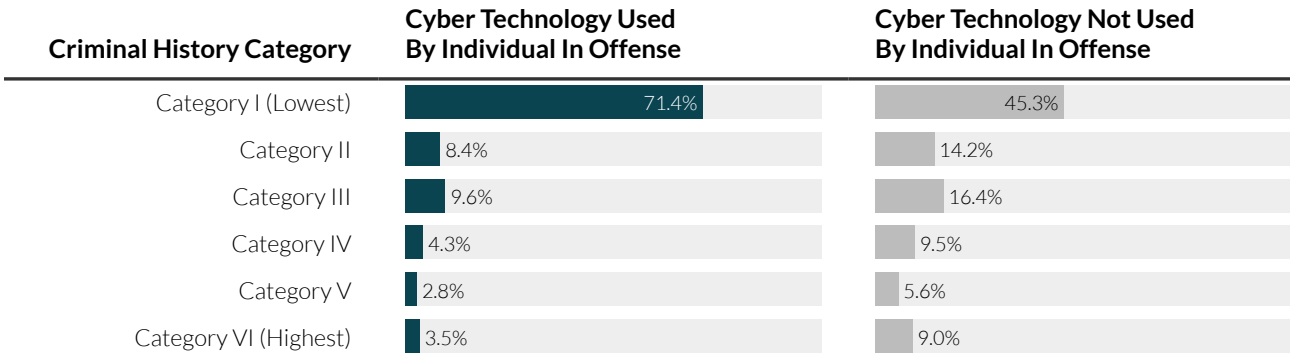
Among individuals sentenced for fraud, money laundering, drug trafficking, and child pornography, those who used cyber technology in the commission of those crimes were younger than other sentenced individuals who committed the same crime. Individuals sentenced for drug trafficking who used cyber technology in the commission of that crime were just over three times more likely to be White compared to others sentenced for drug trafficking (74.0% vs. 24.0%). Individuals sentenced for money laundering who used cyber technology in the commission of that crime were twice as likely to be White compared to others sentenced for money laundering (66.7% vs. 33.6%), while individuals who used cyber technology while committing fraud were also more likely to be White than other individuals sentenced for fraud (52.0% vs. 41.9%). Individuals who used cyber technology in the commission of a fraud, money laundering, or drug trafficking offense were also considerably more likely to be male than other individuals sentenced for these crimes. Individuals who used cyber technology in their crimes were also more likely to have a bachelor's degree compared to those who did not, especially those who were sentenced for drug trafficking (16.2% vs. 3.1%) or money laundering (28.4% vs. 19.4%).

Criminal History

Individuals who used cyber technology in the commission of their federal offense had less extensive criminal histories compared to those who did not use these technologies. The considerable majority (71.4%) were in CHC I, the least serious category, compared to almost half (45.3%) of other sentenced individuals. Only 3.5 percent of individuals who used cyber technology were in CHC VI, the most serious category, while 9.0 percent of the other individuals were in the highest category.

Individuals who used cyber technology in the commission of their federal offense had less extensive criminal histories compared to those who did not use these technologies.

Figure 8. Criminal History Category by Use of Cyber Technology, Fiscal Years 2014–2021



The following sections will discuss each type of cybertechnology, including the number of individuals who used the technology and the types of offenses committed by these individuals.

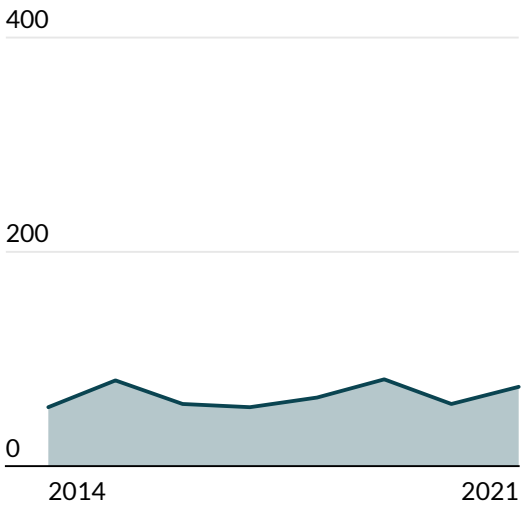
Hacking

The creation or use of computer code in addition to phishing schemes and brute force attacks, including sophisticated hacks involving programming and lower tech hacks.

Trends

Between fiscal years 2014 and 2021, 525 individuals used hacking techniques in the commission of their federal offense. There was not a discernible trend during this time-period. The number of sentenced individuals who used hacking techniques ranged from a low of 55 in fiscal years 2014 and 2017 to a high of 81 in fiscal year 2019.

Figure 9. Hacking Crime Trends, Fiscal Years 2014–2021



Crime Types

A substantial majority of individuals who used hacking techniques in the commission of a federal offense were convicted of a financial crime. Fraud was the most common offense (77.7%) followed by money laundering (6.9%), stalking/harassing (5.0%), and sexual abuse (3.3%).

Figure 10. Federal Crimes Using Hacking Assistance, Fiscal Years 2014–2021[16]

Crime Type	Percent
Fraud/Theft	77.7%
Money Laundering	6.9%
Stalking/Harassing	5.0%
Sexual Abuse	3.3%
Extortion/Racketeering	2.1%
Child Pornography	1.9%
Other	3.1%

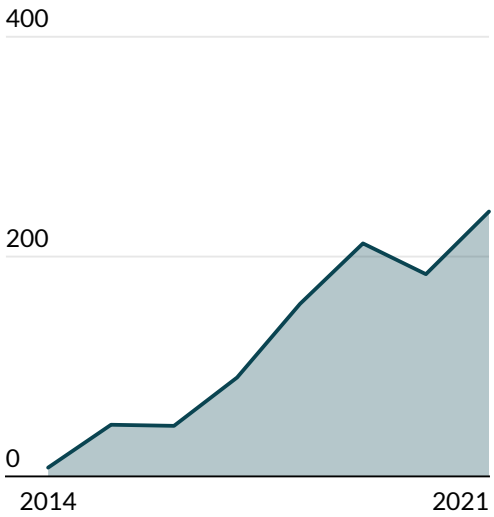
Cryptocurrency

The broad name for digital currencies that use blockchain technology to work on a peer-to-peer basis. Cryptocurrencies do not need a bank to carry out transactions between individuals. The cryptocurrency network keeps track of all the transactions and ensures that no one reneges on a transaction.

Trends

Between 2014 and 2021, 985 sentenced individuals used cryptocurrency in the commission of their offense. The use of cryptocurrency to commit crime increased substantially from 2014 to 2021. In 2014, eight individuals used cryptocurrency in the commission of their offense. In 2015, this number increased to 47, and in 2021, reached a high of 241 individuals.

Figure 11. Cryptocurrency Crime Trends, Fiscal Years 2014–2021



Crime Types

Individuals who used cryptocurrency were convicted of a wide variety of offenses. The most common type of crime committed by individuals using cryptocurrency was drug trafficking (39.6%), followed by fraud (25.3%), and money laundering (19.7%). Child pornography and sexual abuse were committed by 4.1 percent and 2.6 percent, respectively.

Figure 12. Federal Crimes Using Cryptocurrency Assistance, Fiscal Years 2014–2021[17]

Crime Type	Percent
Drug Trafficking	39.6%
Fraud/Theft	25.3%
Money Laundering	19.7%
Child Pornography	4.1%
Sexual Abuse	2.6%
Firearms	2.1%
National Defense	1.5%
Forgery/Counterfeit/Copyright	1.0%
Other	4.2%

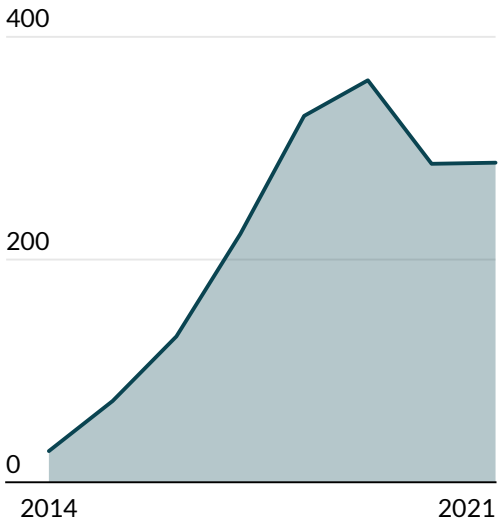
Dark Web

A part of the internet located beyond the reach of traditional internet browsers. It is accessible only through the use of special software and is designed to allow users and website operators to remain anonymous and difficult to trace.

Trends

Between fiscal years 2014 and 2021, 1,718 sentenced individuals used the dark web in the commission of their offense. The number of individuals using the dark web to commit an offense increased from 28 individuals in 2014 to 361 in fiscal year 2019, the year before the COVID-19 pandemic impacted the federal caseload. A total of 286 and 287 individuals who used the dark web in their offense were sentenced in fiscal years 2020 and 2021, respectively.

Figure 13. Dark Web Crime Trends, Fiscal Years 2014–2021



Crime Types

Individuals who used the dark web in the commission of their federal offense were more likely to be sentenced for child pornography than other sentenced individuals. More than 40 percent (42.7%) were sentenced for child pornography. Approximately a quarter (25.7%) were sentenced for drug trafficking, followed by fraud (11.2%), sexual abuse (8.3%), and money laundering (5.8%).

Figure 14. Federal Crimes Using Dark Web Assistance, Fiscal Years 2014–2021[18]

Crime Type	Percent
Child Pornography	42.7%
Drug Trafficking	25.7%
Fraud/Theft	11.2%
Sexual Abuse	8.3%
Money Laundering	5.8%
Firearms	2.0%
National Defense	0.9%
Forgery/Counterfeit/Copyright	0.9%
Other	2.5%

Guideline Application & Sentencing

This section provides information on the application of the sentencing guidelines and the sentences ultimately imposed in cases involving individuals who used cyber technology in their offense compared to other individuals. In particular, information is provided on final offense levels, guideline minimums, and the sentences imposed.[19] While there are no enhancements in the federal sentencing guidelines that specifically address the use of cryptocurrency or the dark web, there are enhancements that may apply more often to individuals who use those technologies or hacking techniques.

Individuals who used cyber technology committed different offenses than other sentenced individuals. For example, individuals sentenced for immigration offenses comprised approximately one-third (33.1%) of other sentenced individuals between fiscal years 2014 and 2021, while only four of the 2,590 individuals who used cyber technology were sentenced for an immigration offense. The analysis that follows compares the guideline application and sentencing outcomes between individuals who used cyber technology and other individuals sentenced for fraud, money laundering, drug trafficking, and child pornography offenses, the four most common offenses committed by those who used cyber technology in the commission of their federal offenses.

Fraud

Overall, individuals sentenced for fraud who used cyber technology had significantly higher average guideline minimums, and in turn, longer sentences imposed than those who did not use cyber technology. Their average guideline minimum was 54 months, 23 months higher than other individuals sentenced for fraud. The average sentence imposed was 36 months for individuals sentenced for fraud who used cyber technology, 14 months higher than for other individuals sentenced for fraud.

While there are no enhancements in the federal sentencing guidelines that specifically address the use of cryptocurrency or the dark web, there are enhancements that may apply more often to individuals who use those technologies or hacking techniques.

Almost two-thirds (63.0%) of individuals sentenced for fraud who used cyber technology were sentenced below the guideline range, compared to 53.8 percent of individuals sentenced for fraud who did not use cyber technology in their offense. The within range rate for those who used cyber technology was 35.1 percent and the above range rate was 1.8 percent. Among individuals sentenced for fraud who did not use cyber technology, the within range rate was 43.9 percent and the above range rate was 2.3 percent.

There was a difference in the enhancement received for loss amount between individuals sentenced for fraud who used cyber technology in their offense and those who did not. The median loss enhancement for those who used cryptocurrency, the dark web, or hacking was ten levels, compared to eight levels for other individuals sentenced for fraud. The loss calculation is the primary driver of the guideline calculation under §2B1.1.[20]

Additionally, individuals sentenced for fraud who used cyber technology were more likely to receive certain enhancements under the §2B1.1 guideline. As noted earlier, while there are no specific enhancements that address the misuse of cryptocurrency or the dark web, five enhancements may be more likely to apply to individuals who use cyber technology and techniques than other individuals sentenced for fraud. Notably, just over half (52.1%) of those who used cyber technology received an enhancement under §2B1.1(b)(10), which provides for a 2-level increase if the defendant used sophisticated means, committed the fraud at least in part outside of the United States, or relocated to evade law enforcement.[21] In contrast, only 15.3 percent of other fraud individuals received this enhancement.

Figure 15. Sentencing Statistics by Use of Cyber Technology in Fraud, Fiscal Years 2014–2021

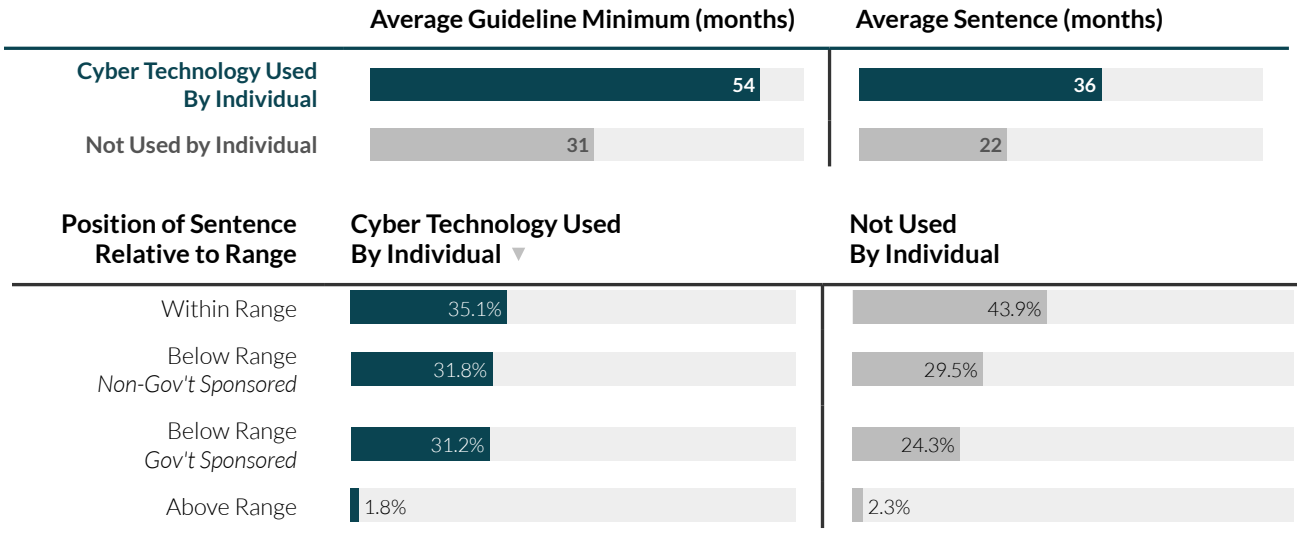
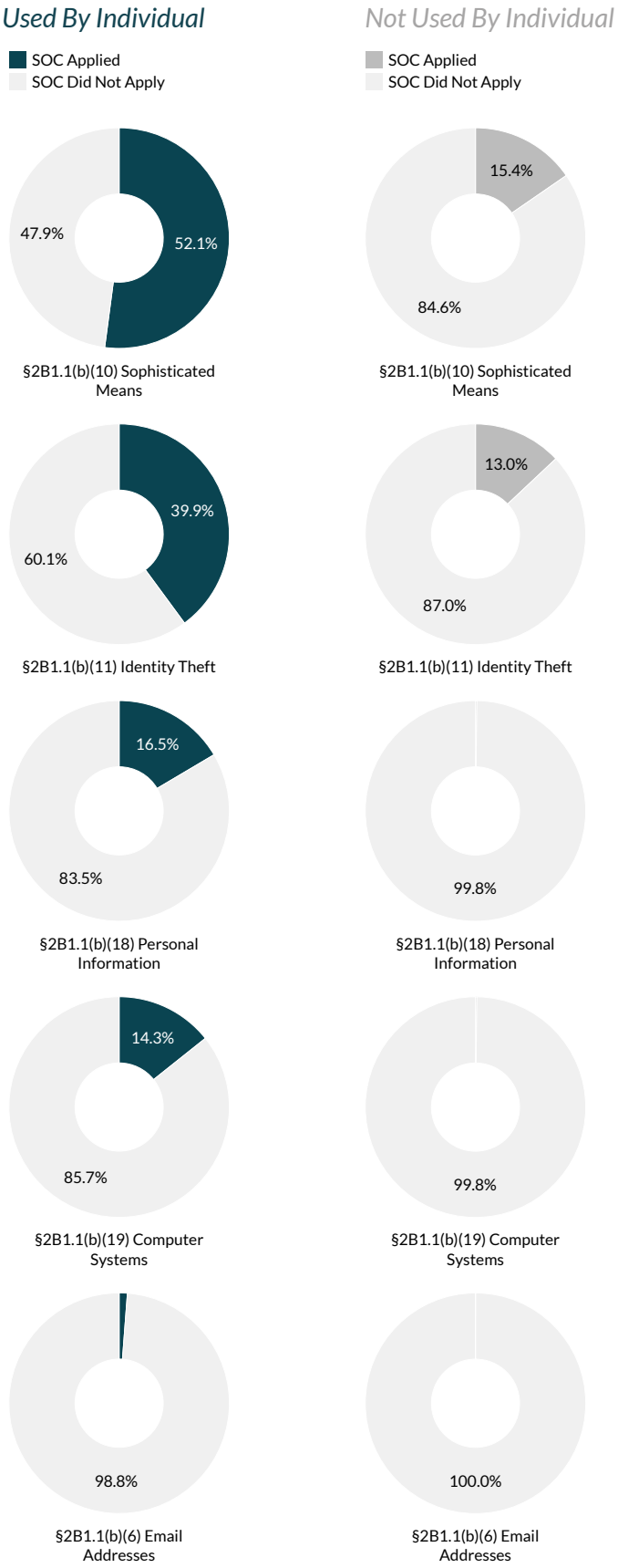


Figure 16. Fraud Enhancements (§2B1.1) by Use of Cyber Technology, Fiscal Years 2014–2021



A sizeable share (39.9%) of individuals who used cyber technology and were sentenced for fraud received an enhancement at §2B1.1(b)(11) for identity theft.[22] In contrast, only 13.0 percent of other individuals sentenced for fraud received this 2-level increase. Relatedly, those who used cyber technology were also considerably more likely to receive the 2-level enhancement at §2B1.1(b)(18) for intent to obtain personal information or the unauthorized dissemination of personal information than other individuals (16.5% compared to 0.2%).[23]

A 2- to 18-level enhancement at §2B1.1(b)(19) applied if the offense involved a computer system used to maintain or operate critical infrastructure or used by a government entity in furtherance of the administration of justice, national defense, or national security.[24] This enhancement applied in 14.3 percent of cyber technology sentencings compared to only 0.2 percent of other individuals sentenced for fraud.

Lastly, individuals who used cyber technology were more likely to receive a rarely used 2-level enhancement at §2B1.1(b)(6) for obtaining email addresses through improper means.[25] While 1.2 percent of these individuals received this enhancement, 0.01 percent of other individuals sentenced for fraud received it.

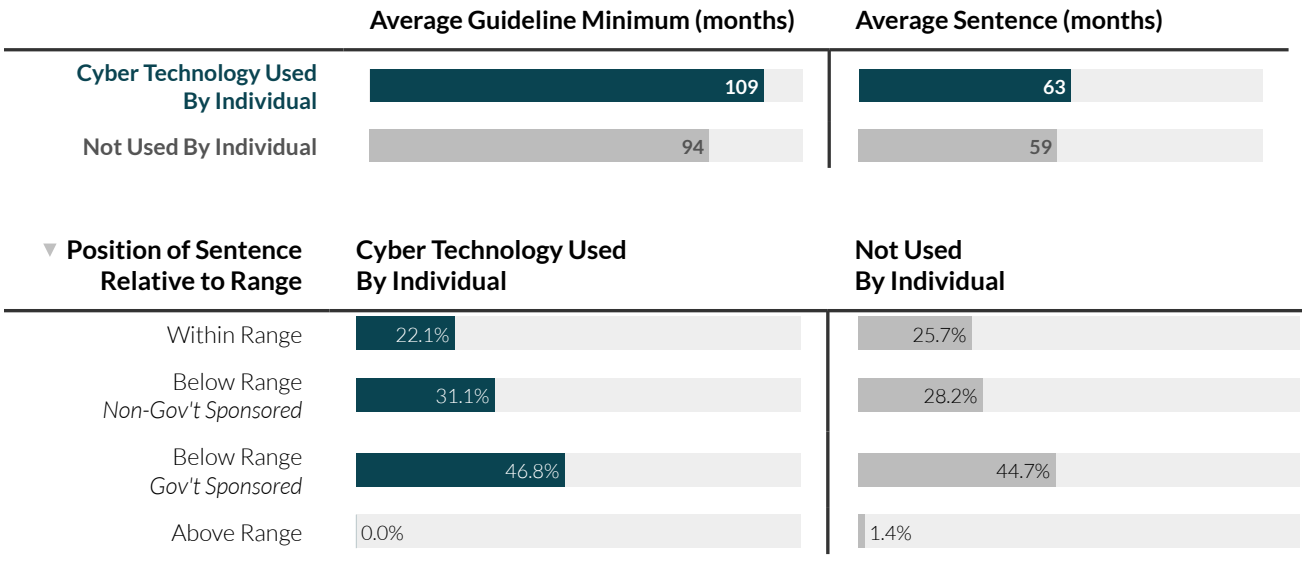
Money Laundering

The average guideline minimum and average sentence imposed were higher for individuals sentenced for money laundering who exploited cyber technology compared to others sentenced for money laundering. Those who used cyber technology had a guideline minimum of 109 months, 15 months higher than other individuals sentenced for money laundering of 94 months. The average sentence imposed was 63 months for individuals sentenced for money laundering who used cyber technology compared to 59 months for others sentenced for money laundering.

A substantial majority of both groups sentenced for money laundering were sentenced below the guideline range. Among those who used cyber technology, 77.9 percent were sentenced below the range and 72.9 percent of those who did not use cyber technology were sentenced below the range. In addition, a similar proportion of those who used cyber technology were sentenced within the range as others sentenced for money laundering (22.1% and 25.7%, respectively). No individuals who used cyber technology were sentenced above the range compared to 1.4 percent of others sentenced for money laundering.

Individuals sentenced for money laundering who used cyber technology had a lower median loss enhancement than others sentenced for money laundering. Those who used cyber technology had a median loss of ten compared to 12 for individuals sentenced for money laundering who did not use cyber technology.

Figure 17. Money Laundering Sentencing Statistics by Use of Cyber Technology, Fiscal Years 2014–2021



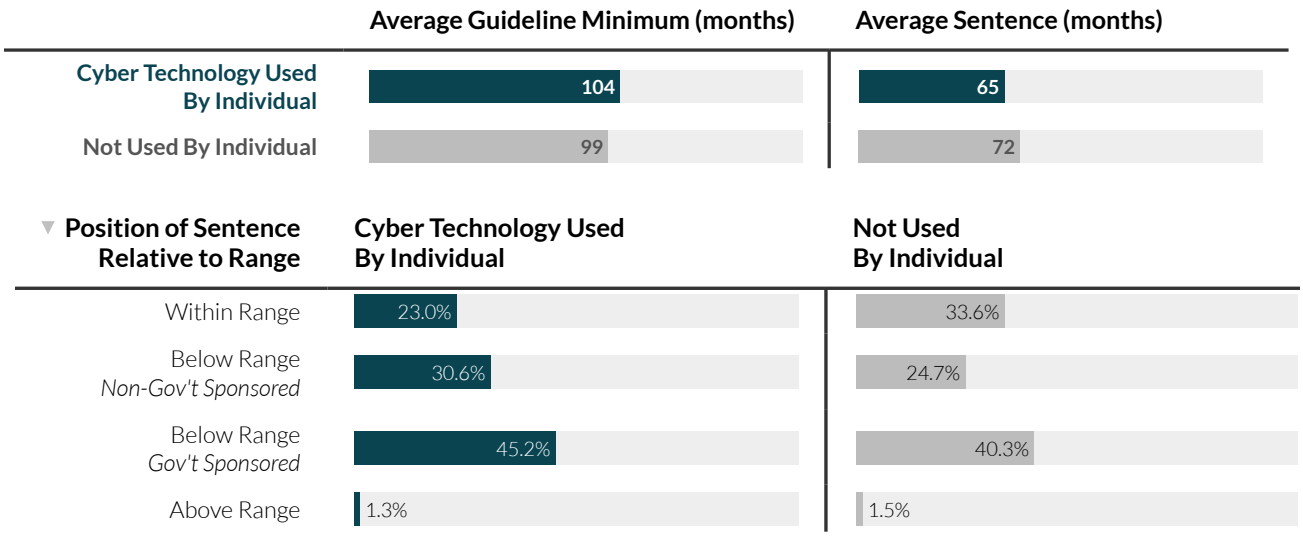
Additionally, a 2-level enhancement at §2S1.1(b)(3) for sophisticated laundering was applied more often to those who used cyber technology than to others sentenced for money laundering.[26] The sophisticated laundering enhancement applied to 21.8 percent of individuals who used cyber technology compared to 7.1 percent of other individuals sentenced under this guideline.

Drug Trafficking

Individuals sentenced for drug trafficking who used cyber technology had a higher average guideline minimum than others sentenced for drug trafficking, but a lower average sentence imposed. The average guideline minimum for those using cyber technology was 104 months compared to 99 months for all other persons sentenced for drug trafficking. The average sentence imposed was 65 months for those who used cyber technology, which was seven months lower than the average sentence of 72 months imposed on others sentenced for drug trafficking.

Individuals sentenced for drug trafficking who used cyber technology were more likely to be sentenced below the guideline range. About three-quarters (75.8%) of individuals who used cyber technology were sentenced below the range compared to 65.0 percent of others sentenced for drug trafficking. Consequently, the within range rate was about ten percentage points lower for those who used cyber technology compared to others sentenced for drug trafficking (23.0% vs. 33.6%). The above range rates were similar, at 1.3 percent for those who used cyber technology and 1.5 percent for others sentenced for drug trafficking.

Figure 18. Drug Trafficking Sentencing Statistics by Use of Cyber Technology, Fiscal Years 2014–2021

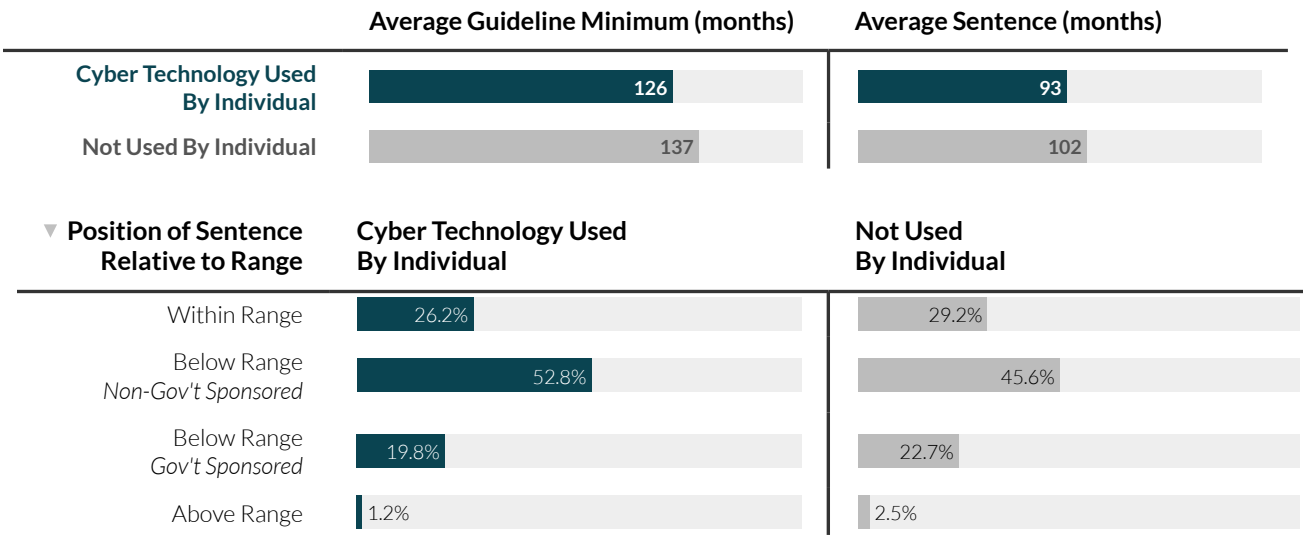


Child Pornography

The average guideline minimum and average sentence imposed were lower for individuals sentenced for child pornography who used cyber technology compared to other individuals sentenced for those offenses. These individuals had a guideline minimum of 126 months compared to 137 months for others sentenced for child pornography. The average sentence imposed was 93 months for those sentenced for child pornography who used cyber technology compared to 102 months for others sentenced for child pornography. While those who used cyber technology in their offense had the same final offense level as other individuals sentenced for child pornography, they had a slightly lower criminal history.

Among individuals sentenced for child pornography who used cyber technology, 72.6 percent were sentenced below the guideline range compared to 68.3 percent of those who did not use cyber technology in their offense. A similar proportion of individuals who used cyber technology were sentenced within the range as other individuals who were sentenced for child pornography (26.2% and 29.2%, respectively). The above range rate was 1.2 percent for these individuals and 2.5 percent for others who were sentenced for child pornography.

Figure 19. Child Pornography Sentencing Statistics by Use of Cyber Technology, Fiscal Years 2014–2021



Conclusion

During the time period studied, individuals sentenced in federal court used cyber technologies involving hacking techniques, cryptocurrency, and the dark web at an increasing rate to commit their federal offense. These technologies facilitate a wide variety of criminal activity. They also can help conceal this activity and present challenges in the investigation and prosecution of these crimes. This report provides the Commission's first detailed analysis on the use of cyber technology in federal crime.

Cyber technology contributes to a variety of federal crimes. As demonstrated in this report, fraud, drug trafficking, child pornography, and money laundering were the most common offenses in which a cyber technology was used. The type of technology used varied by type of offense.

Sentenced individuals who used cyber technology differed from the remaining sentenced individuals in the federal population. Individuals who use cyber technology to engage in criminal activity are more likely to be younger, White, male, and have a college degree than other sentenced individuals. They were also more likely to have little or no criminal history compared to others.

Within the same crime type, individuals who used cyber technology or techniques differed from those who did not use these technologies. Those who used cyber technology or techniques to commit fraud or money laundering were more likely to receive certain sentencing enhancements than other individuals sentenced for those offenses. In particular, those individuals were more likely to receive enhancements related to sophisticated means/sophisticated laundering than other individuals convicted of such offenses, as well as enhancements related to identity theft and computer intrusion.

Endnotes

1 Off. of the Inspector Gen., U.S. Dep't of Just., Audit of the Federal Bureau of Investigation's Strategy and Efforts to Disrupt Illegal Dark Web Activities, at i (2020) [hereinafter OIG Audit] ("Many users access the dark web for legitimate purposes, including to discuss socially sensitive matters or counter censorship in oppressive areas of the world. However, dark web sites are also used to engage in illegal activities, such as trafficking drugs; firearms and weapons of mass destruction; child sexual abuse material; malware; and other illicit goods and services. According to the Department [of Justice], the existence of darknet marketplaces is one of the greatest impediments to its efforts to disrupt cybercriminal activities.").

2 Off. of the Deputy Att'y Gen., U.S. Dept of Justice, Cryptocurrency Enforcement Framework 5-6 (2020) [hereinafter Cryptocurrency Enforcement Report].

3 *Id.*

4 Interpol, National Cybercrime Strategy Guidebook 15 (2021) ("Cybercrime frequently involves cross-border investigations as victims, offenders and infrastructure can be in different countries. This poses a challenge for investigators as they often discover that other countries may not have the same laws that criminalize the offence, or there are differing elements needed to prove the offence has taken place or that there are varying data retention periods for subscriber data. In some countries, there may even be a lack of legislation and therefore criminalization of cybercrime, which creates a situation where the country becomes a safe haven for cybercriminals.").

5 *See* Internet Crime Complaint Ctr., Fed. Bureau of Investigation, Internet Crime Report 2021 (2022); Fin. Crimes Enf't Network, U.S. Dep't of Treasury, Financial Trend Analysis: Ransomware Trends in Bank Secrecy Act Data Between July 2021 and December 2021 (2021).

6 Reference to sentencing years in this report refer to fiscal years.

7 To fulfill its statutory responsibilities, the Commission collects and analyzes data on federal sentences for every federal felony and Class A misdemeanor individual sentenced each year. Courts are statutorily required to submit five sentencing documents to the Commission within 30 days of entry of judgment in a criminal case: (1) the charging document; (2) the plea agreement (if applicable); (3) the Presentence Report; (4) the Judgment and Commitment Order; and (5) the Statement of Reasons form. *See* 28 U.S.C. § 994(w)(1). The Commission routinely extracts and codes data from these documents, including sentencing data, demographic variables, statutory information, guideline application decisions, and departure and variance information. See the Appendix for more information on the methodology of the special coding project used for this report.

8 There is no agreement as to what activities are included in the definition of hacking. This report includes illegal activities which impede at least one of the three pillars of information security: confidentiality, integrity, or availability. Nat'l Inst. of Standards & Tech., Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events 1 (2020).

Various activities such as hacking, phishing, brute force attacks, and Distributed Denial of Service Attacks as defined by the Commission are included for the purposes of this report. U.S. Sent'g Comm'n, Hacking & Phishing Glossary: 2018 Annual National Seminar 2 (2018). Commission materials cited herein are available on the Commission's website at www.ussc.gov.

9 Blockchain technology is a digital file distributed to everyone participating in a cryptocurrency network. The blockchain acts as a general ledger and keeps track of all the transactions that happen in a network. Everyone can see what transactions have happened on the network and the blockchain is sealed using cryptography so that no one can tamper with it. U.S. Sent'g Comm'n, *Glossary of Federal Sentencing-Related Terms*, https://www.ussc.gov/education/glossary (last visited Aug. 29, 2024).

10 *Id.* (defining the term cryptocurrency).

11 *Id.*

12 "Cryptocurrency is a form of virtual asset that uses cryptography to secure financial transactions. Many of cryptocurrency's central features—including decentralized operation and control, and, in some cases, a high degree of anonymity—present new and unique challenges for public safety that must be addressed, lest the technology be used predominantly for criminal activity." Cryptocurrency Enforcement Report, *supra* note 2, at 1.

13 "The terms 'dark web' and 'darknet' are often used to refer to a part of the Internet that consists of services and websites that cannot be accessed through standard web browsers; instead, specific software, configurations, or authorization is needed for access. While accessing the dark web is not illegal, dark web sites are often used to engage in illegal activities." OIG Audit, *supra* note 1.

14 The definitions of the Commission's crime type categories can be found in Appendix A at U.S. Sent'g Comm'n, 2021 Sourcebook of Federal Sentencing Statistics app. A, at 197–213 (2022).

15 "Other" includes primary offense types with fewer than ten individuals. Offenses include drug possession, administration of justice, bribery/corruption, immigration, assault, commercialized vice, food and drug, individual rights, tax, environmental, murder, arson, burglary/trespassing, obscenity/other sex offenses, and prison offenses.

16 "Other" includes primary offense types with fewer than ten individuals. Offenses include drug possession, administration of justice, bribery/corruption, immigration, assault, commercialized vice, food and drug, individual rights, tax, environmental, murder, arson, burglary/trespassing, obscenity/other sex offenses, and prison offenses.

17 "Other" includes primary offense types with fewer than ten individuals. Offenses include drug possession, administration of justice, bribery/corruption, immigration, assault, commercialized vice, food and drug, individual rights, tax, environmental, murder, arson, burglary/trespassing, obscenity/other sex offenses, and prison offenses.

18 "Other" includes primary offense types with fewer than ten individuals. Offenses include drug possession, administration of justice, bribery/corruption, immigration, assault, commercialized vice, food and drug, individual rights, tax, environmental, murder, arson, burglary/trespassing, obscenity/other sex offenses, and prison offenses.

19 The final offense level is determined by taking the base offense level and then adding or subtracting from it any specific offense characteristics and adjustments that may apply. The final offense level along with the sentenced individual's criminal history category determine the individual's guideline range. *See generally* U.S. Sent'g Comm'n, Overview of the Federal Sentencing Guidelines 2 (2022).

20 U.S. Sent'g Comm'n, Guidelines Manual §2B1.1 (Nov. 2023) [hereinafter USSG].

21 USSG §2B1.1(b)(10)(A)-(C).

22 USSG §2B1.1(b)(11)(A)-(C).

23 USSG §2B1.1(b)(18)(A)-(B).

24 USSG §2B1.1(b)(19)(A)-(B).

25 USSG §2B1.1(b)(6)(A)-(B).

26 USSG §2S1.1(b)(3)(A)-(B).

Appendix

This Appendix provides the search terms used to identify cases for review. For some terms listed below, varying versions of the term were included in the search. For example, to search for "Bitcoin" the terms "Bitcoin, bit coin, bit-coin" were included. The search term "crypto" captured every word that had "crypto" in the word. For each identified case, the PSR, plea, and indictment were read by staff to determine if there was any indication that cyber technology was used by the sentenced individual. If so, the type of cyber technology used by the individual was coded.

Hacking Terms

Hacked, Hacking, Hacker, Hactivist, Cyberattack, Keylogger, Malware, Trojan horse, Data breach, DDoS, Distributed denial of service, Wannacry, Lulzsec, Packet sniffer, Botnet, Jackpotting, Ransomware, Phishing

Cryptocurrency Terms

Crypto, Bitcoin, Blockchain, Initial coin offerings, Ethereum, Altcoin, Litecoin

Dark Web Terms

Dark web, Darknet, Deep Web, Tor browser, Onion router, Silk Road, Alpha Bay, Operation Pacifier

United States Sentencing Commission
www.ussc.gov

THURGOOD MARSHALL FEDERAL JUDICIARY BUILDING
ONE COLUMBUS CIRCLE N.E.
SUITE 2-500, SOUTH LOBBY
WASHINGTON, DC 20002-8002

This document was produced and published at U.S. taxpayer expense.