COMMONWEALTH OF PENNSYLVANIA
COUNTY OF:DAUPHIN

Magisterial District Number: 12-2-05
MDJ: Hon. Paul T. Zozos
Address: 1300 Rolleston Street
Harrisburg, PA 17104

Telephone: (717)234-0949

POLICE CRIMINAL COMPLAINT
COMMONWEALTH OF PENNSYLVANIA
VS.

DEFENDANT: *(NAME and ADDRESS):*

TYREESE *First Name* | L. *Middle Name* | LEWIS *Last Name* | Ge

821 Squire Road
Harrisburg, PA 17111

NCIC Extradition Code Type

- ☒ 1-Felony Full
- ☐ 2-Felony Limited
- ☐ 3-Felony Surrounding States
- ☐ 4-Felony No Extradition
- ☐ 5-Felony Pending Extradition
- ☐ 6-Felony Pending Extradition Determ.
- ☐ A-Misdemeanor Full
- ☐ B-Misdemeanor Limited
- ☐ C-Misdemeanor Surrounding States
- ☐ D-Misdemeanor No Extradition
- ☐ E-Misdemeanor Pending Extradition
- ☐ F-Misdemeanor Pending Extradition
- ☐ Distance: _____

DEFENDANT IDENTIFICATION INFORMATION

Docket Number	Date Filed	OTN/LiveScan Number	Complaint/Incident Number	Request Lab Services?
CR-319-23	07/26/2023	R515432-1	FCC-22-0014	☐ YES ☐ NO

GENDER	DOB	POB	Add'l DOB	Co-Defendant(s)
☒ Male ☐ Female	12/25/2000		/ /	☐

First Name	Middle Name	Last Name	Gen.
AKA			

RACE ☐ White ☐ Asian ☒ Black ☐ Native American ☐ Unknown

ETHNICITY ☐ Hispanic ☐ Non-Hispanic ☐ Unknown

Hair Color
☐ GRY (Gray) ☐ RED (Red/Aubn.) ☐ SDY (Sandy) ☐ BLU (Blue) ☐ PLE (Purple) ☐ BRO (Brown)
☒ BLK (Black) ☐ ONG (Orange) ☐ WHI (White) ☐ XXX (Unk./Bald) ☐ GRN (Green) ☐ PNK (Pink)
☐ BLN (Blonde / Strawberry)

Eye Color
☐ BLK (Black) ☐ BLU (Blue) ☒ BRO (Brown) ☐ GRN (Green) ☐ GRY (Gray)
☐ HAZ (Hazel) ☐ MAR (Maroon) ☐ PNK (Pink) ☐ MUL (Multicolored) ☐ XXX (Unknown)

DNA	☐ YES ☐ NO	DNA Location	WEIGHT (lbs.)
FBI Number		MNU Number	
Defendant Fingerprinted	☐ YES ☐ NO		Ft. HEIGHT In.
Fingerprint Classification:			

DEFENDANT VEHICLE INFORMATION

Plate #	State	Haz mat	Registration Sticker (MM/YY) /	Comm'l Veh. Ind. ☐	School Veh. ☐	Oth. NCIC Veh. Code	Reg. same as Def. ☐

VIN	Year	Make	Model	Style	Color

Office of the attorney for the Commonwealth ☒ Approved ☐ Disapproved because: _____

(The attorney for the Commonwealth may require that the complaint, arrest warrant affidavit, or both be approved by the attorney for the Commonwealth prior to filing. See Pa.R.Crim.P. 507).

PATRICK SCHULTE, CDAG
(Name of the attorney for the Commonwealth)

Approved via Prime
(Signature of the attorney for the Commonwealth)

07/26/2023
(Date)

I, KATHRYN GRADY AND CHRISTOPHER COLARUSSO (Name of the Affiant) OAG BADGE 797 / PSP BADGE 8789 (PSP/MPOETC -Assigned Affiant ID Number & Badge #)

of Pennsylvania Office of Attorney General (Identify Department or Agency Represented and Political Subdivision) PA0222400 (Police Agency ORI Number)

do hereby state: (check appropriate box)

1. ☒ I accuse the above named defendant who lives at the address set forth above
   ☐ I accuse the defendant whose name is unknown to me but who is described as _____

   ☐ I accuse the defendant whose name and popular designation or nickname are unknown to me and whom I have therefore designated as John Doe or Jane Doe

   with violating the penal laws of the Commonwealth of Pennsylvania at [301] (Subdivision Code) Harrisburg City (Place-Political Subdivision)

   in DAUPHIN County [22] (County Code) on or about JANUARY 1, 2022 THROUGH PRESENT

POLICE CRIMINAL COMPLAINT

Docket Number:	Date Filed:	OTN/LiveScan Number	Complaint/Incident Number
CR-319-23	7 AUG 23	R515432-1	FCC-22-0014

Defendant Name:	First:	Middle:	Last:
	TYREESE		LEWIS

The acts committed by the accused are described below with each Act of Assembly or statute allegedly violated, if appropriate. When there is more than one offense, each offense should be numbered chronologically.

(Set forth a *brief* summary of the facts sufficient to advise the defendant of the nature of the offense(s) charged. A citation to the statute(s) allegedly violated, without more, is not sufficient. In a summary case, you must cite the specific section(s) and subsection(s) of the statute(s) or ordinance(s) allegedly violated. The age of the victim at the time of the offense may be included if known. In addition, social security numbers and financial information (e.g. PINs) should not be listed. If the identity of an account must be established, list only the last four digits. 204 PA.Code §§ 213.1 – 213.7.)

Inchoate Offense ☐ **Attempt** *18 901 A* ☐ **Solicitation** *18 902 A* ☐ **Conspiracy** *18 903*

Number of Victims Age 60 or Older _____

Lead?	Offense #	Section	Subsection		PA Statute (Title)	Counts	Grade	NCIC Offense Code	UCR/NIBRS Code
☒	1	911	B3	of the	18 PA C.S.A.	1	F1		

PennDOT Data (if applicable) Accident Number _____ ☐ Interstate ☐ Safety Zone ☐ Work Zone

Statute Description (include the name of statute or ordinance): **CORRUPT ORGANIZATIONS**

Acts of the accused associated with this Offense: In that the Defendant being employed by or associated with an enterprise, conducted or participated, directly or indirectly, in the conduct of such enterprise's affairs through a pattern of racketeering activity, that is, during the periods as set forth herein. TO WIT: Tyreese Lewis and his co-conspirators, while associated with an enterprise, conducted and/or participated, directly or indirectly, in the conduct of the enterprise's affairs through a pattern of Dealing in Proceeds of Unlawful Activities, Theft by Unlawful Taking, Theft by Deception, Access Device Fraud, and/or Identity Theft.

Inchoate Offense ☐ **Attempt** *18 901 A* ☐ **Solicitation** *18 902 A* ☒ **Conspiracy** *18 903*

Number of Victims Age 60 or Older _____

Lead?	Offense#	Section	Subsection		PA Statute (Title)	Counts	Grade	NCIC Offense Code	UCR/NIBRS Code
☐	2	911	B4	of the	18 PA C.S.A.	1	F1		

PennDOT Data (if applicable) Accident Number _____ ☐ Interstate ☐ Safety Zone ☐ Work Zone

Statute Description (include the name of statute or ordinance): **CONSPIRACY - CORRUPT ORGANIZATION**

Acts of the accused associated with this Offense: In that the Defendant, while employed by or associated with an enterprise, conspired to conduct or participate, directly or indirectly, in the conduct of such enterprise's affairs through a pattern of racketerring activity. TO WIT: Tyreese Lewis and his co-conspirators to participate in the conduct of the enterprise's affairs through a pattern of Dealing in Proceeds of Unlawful Activities, Theft by Unlawful Taking, Theft by Deception, Access Device Fraud, and/or Identity Theft.

Inchoate Offense ☐ **Attempt** *18 901 A* ☐ **Solicitation** *18 902 A* ☐ **Conspiracy** *18 903*

Number of Victims Age 60 or Older _____

Lead?	Offense#	Section	Subsection		PA Statute (Title)	Counts	Grade	NCIC Offense Code	UCR/NIBRS Code
☐	3	5111	A2	of the	18 PA C.S.A.	1			

PennDOT Data (if applicable) Accident Number _____ ☐ Interstate ☐ Safety Zone ☐ Work Zone

Statute Description (include the name of statute or ordinance): **DEALING IN PROCEEDS OF UNLAWFUL ACTIVTIES**

Acts of the accused associated with this Offense: In that the Defendant, conducts a financial transaction with knowledge that the property involved, including stolen or illegally obtained property, represents the proceeds of unlawful activity and that the transaction is designed in whole or in part to conceal or disguise the nature, location, source, ownership or conrol of the proceeds of unlawful activity. TO WIT: Tyreese Lewis and his co-conspirators participated in the movement of funds between multiple accounts, which included accounts in the names of Identity Theft victims, to conceal to the source of the fraudulent funds. Lewis and his co-conspirators, with intent, to conceal the movement of stolen funds from the victims accounts through the use of cash advances, gift card purchases, western union transfers, and peer-to-peer transactions in ficitious names.

POLICE CRIMINAL COMPLAINT

Docket Number:	Date Filed:	OTN/LiveScan Number	Complaint/Incident Number
CR-319-23	7/24/23	K 515432-1	FCC-22-0014

Defendant Name:	First:	Middle:	Last:
	TYREESE		LEWIS

Inchoate Offense ☐ Attempt *18 901 A* ☐ Solicitation *18 902 A* ☐ Conspiracy *18 903* — **Number of Victims Age 60 or Older** _____

Lead?	Offense#	Section	Subsection		PA Statute (Title)	Counts	Grade	NCIC Offense Code	UCR/NIBRS Code
☐	4	4120		of the	18 PA C.S.A.	1	F3		

PennDOT Data (if applicable) Accident Number _____ ☐ Interstate ☐ Safety Zone ☐ Work Zone

Statute Description (include the name of statute or ordinance): **IDENTITY THEFT**

Acts of the accused associated with this Offense: In that the Defendant, possesses or uses, through any means, identifying information of another person without the consent of that other person to further any unlawful purpose. TO WIT: Tyreese Lewis and his co-conspirators purchased the identities of victims online and used the information to take over bank accounts at multiple financial institutions to initatie fraudulent transfers from the victim accounts. In adition, Lewis and his co-conspirators shared or sold the victim identities with each other and other unidentified co-conspirators.

Inchoate Offense ☐ Attempt *18 901 A* ☐ Solicitation *18 902 A* ☐ Conspiracy *18 903* — **Number of Victims Age 60 or Older** _____

Lead?	Offense#	Section	Subsection		PA Statute (Title)	Counts	Grade	NCIC Offense Code	UCR/NIBRS Code
☐	5	3921	A	of the	18 PA C.S.A.	1	F1		

PennDOT Data (if applicable) Accident Number _____ ☐ Interstate ☐ Safety Zone ☐ Work Zone

Statute Description (include the name of statute or ordinance): **THEFT BY UNLAWFUL TAKING OR DISPOSITION**

Acts of the accused associated with this Offense: In that the Defendant, unlawfully took or exercised unlawful control over, movable property of another with intent to deprvie him thereof. TO WIT: Tyreese Lewis and his co-conspirators took control of victim financial accounts through the use of spam phone calls in which they impersonated the financial institutions fraud departments to gain control of the victims online banking. Lewis and his co-conspirators unlawfully accessed the financial accounts of over 400 victims and made fraudulent transfers or purchases with their account information, which totaled approximately $1.8 million dollars in fraudulent transfer of funds.

Inchoate Offense ☒ Attempt *18 901 A* ☐ Solicitation *18 902 A* ☐ Conspiracy *18 903* — **Number of Victims Age 60 or Older** _____

Lead?	Offense#	Section	Subsection		PA Statute (Title)	Counts	Grade	NCIC Offense Code	UCR/NIBRS Code
☐	6	3921	A	of the	18 PA C.S.A.	1	F1		

PennDOT Data (if applicable) Accident Number _____ ☐ Interstate ☐ Safety Zone ☐ Work Zone

Statute Description (include the name of statute or ordinance): **ATTEMPTED THEFT BY UNLAWFUL TAKING OR DISPOSITION**

Acts of the accused associated with this Offense: In that the Defendant, unlawfully took or exercised unlawful control over, movable property of another with intent to deprvie him thereof. TO WIT: Tyreese Lewis and his co-conspirators took control of victim financial accounts through the use of spam phone calls in which they impersonated the financial institutions fraud departments to gain control of the victims online banking. Lewis and his co-conspirators unlawfully accessed the financial accounts of over 400 victims and made fraudulent transfers or purchases with their account information, which totaled approximately $1.8 million in fraudulent transfer of funds. Lewis and his co-conspirators attempted to access and/or make fraudulent purchases with additional victims, but their attempts were unsuccesful.

POLICE CRIMINAL COMPLAINT

Docket Number:	Date Filed:	OTN/LiveScan Number	Complaint/Incident Number
CR-319-23	7/26/23	R515432-1	FCC-22-0014

Defendant Name:	First:	Middle:	Last:
	TYREESE		LEWIS

Inchoate Offense ☐ Attempt *18 901 A* ☐ Solicitation *18 902 A* ☐ Conspiracy *18 903* — **Number of Victims Age 60 or Older** _____

Lead?	Offense#	Section	Subsection		PA Statute (Title)	Counts	Grade	NCIC Offense Code	UCR/NIBRS Code
☐	7	3922	A2	of the	18 PA C.S.A.	1	F1		

PennDOT Data (if applicable) Accident Number _____ ☐ Interstate ☐ Safety Zone ☐ Work Zone

Statute Description (include the name of statute or ordinance): **THEFT BY DECEPTION**

Acts of the accused associated with this Offense: In that the Defendant, did intentionally obtain property of another by deception by creating a false impresion, including false impressions as to law, value, intention or other state of mind. TO WIT: Tyreese Lewis and co-conspirators impersonated the fraud departments of financial institutions in order to gain access to the victim's bank accounts. The victims provided and confirmed their perosnal identifying information and account credentials under the belief they were being contacted by their financial institution. As a result of the activity, Lewis and the co-conspirators were able to steal approximately $1.8 million.

Inchoate Offense ☒ Attempt *18 901 A* ☐ Solicitation *18 902 A* ☐ Conspiracy *18 903* — **Number of Victims Age 60 or Older** _____

Lead?	Offense#	Section	Subsection		PA Statute (Title)	Counts	Grade	NCIC Offense Code	UCR/NIBRS Code
☐	8	3922	A2	of the	18 PA C.S.A.	1	F1		

PennDOT Data (if applicable) Accident Number _____ ☐ Interstate ☐ Safety Zone ☐ Work Zone

Statute Description (include the name of statute or ordinance): **ATTEMPTED THEFT BY DECEPTION**

Acts of the accused associated with this Offense: In that the Defendant did, with intent to commit the crime of Theft By Deception, perofmred an act constituting a substantial step toward the committing of the crime of Theft By Deception. TO WIT: Tyreese Lewis and co-conspirators impersonated the fraud departments of financial institutions in order to gain access to the victim's bank accounts. The victims provided and confirmed their perosnal identifying information and account credentials under the belief they were being contacted by their financial institution. As a result of the activity, Lewis and the co-conspirators were able to steal approximately $1.8 million. In addition, Lewis and the co-conspirators attempted to gain access to additional victim accounts, but were unsuccesful in their attempts to take over the financial account.

Inchoate Offense ☐ Attempt *18 901 A* ☐ Solicitation *18 902 A* ☐ Conspiracy *18 903* — **Number of Victims Age 60 or Older** _____

Lead?	Offense#	Section	Subsection		PA Statute (Title)	Counts	Grade	NCIC Offense Code	UCR/NIBRS Code
☐	9	3925	A	of the	18 PA C.S.A.	1	F1		

PennDOT Data (if applicable) Accident Number _____ ☐ Interstate ☐ Safety Zone ☐ Work Zone

Statute Description (include the name of statute or ordinance): **RECEIVING STOLEN PROPERTY**

Acts of the accused associated with this Offense: In that the Defendant intentionally received, retained, or disposed of movable property of another knowing that it had been stolen, or belieiving that it has probably been stolen, unless the property is received, retained, or disposed with intent to restore it to the owner. TO WIT: Tyreese Lewis and co-conspirators purchased the personal identifying information of over 400 victims and fraudulently accessed the financial accounts and financial instruments and obtained approximately $1.8 million in proceeds.

POLICE CRIMINAL COMPLAINT

Docket Number:	Date Filed:	OTN/LiveScan Number	Complaint/Incident Number
CR-319-23	1/24/23	R515432-1	FCC-22-0014

Defendant Name:	First:	Middle:	Last:
	TYREESE		LEWIS

Inchoate Offense ☐ Attempt *18 901 A* ☐ Solicitation *18 902 A* ☐ Conspiracy *18 903*

Number of Victims Age 60 or Older _____

Lead?	Offense#	Section	Subsection		PA Statute (Title)	Counts	Grade	NCIC Offense Code	UCR/NIBRS Code
☐	10	4106	A1(ii)	of the	18 PA C.S.A.	1	F3		

PennDOT Data (if applicable) Accident Number _____ ☐ Interstate ☐ Safety Zone ☐ Work Zone

Statute Description (include the name of statute or ordinance): **ACCESS DEVICE FRAUD**

Acts of the accused associated with this Offense: In that the defendant, commits an offense if he uses an access device to obtain or in an attempt to obtain property or services with knowledge that the access device was isued to another person who has not authorized its use. TO WIT: Tyreese Lewis and co-conspirators purchased the debit and/or credit card numbers through an online website of over 400 victims who did not have knowledge that their personal identifying information and banking information had been published for sale. As a result of the activity, Tyreese Lewis and his co-conspirators obtained approximately $1.8 million in proceeds.

Inchoate Offense ☐ Attempt *18 901 A* ☐ Solicitation *18 902 A* ☐ Conspiracy *18 903*

Number of Victims Age 60 or Older _____

Lead?	Offense#	Section	Subsection		PA Statute (Title)	Counts	Grade	NCIC Offense Code	UCR/NIBRS Code
☐	11	7615	A4	of the	18 PA C.S.A.	1	F3		

PennDOT Data (if applicable) Accident Number _____ ☐ Interstate ☐ Safety Zone ☐ Work Zone

Statute Description (include the name of statute or ordinance): **COMPUTER TRESPASS**

Acts of the accused associated with this Offense: In that the Defendant, knowingly and without authority or in excess of given authority uses a computer or computer network with the intent to effect the creation or alteration of a financial instrument or of an electronic transfer of funds. TO WIT: Tyreese Lewis and his co-conspirators fraudulently accessed approximately 350 victim accounts and created unauthorized electronic transfers, which totaled approximately $1.6 million.

Inchoate Offense ☐ Attempt *18 901 A* ☐ Solicitation *18 902 A* ☐ Conspiracy *18 903*

Number of Victims Age 60 or Older _____

Lead?	Offense#	Section	Subsection		PA Statute (Title)	Counts	Grade	NCIC Offense Code	UCR/NIBRS Code
☐	12	7512	A	of the	18 PA C.S.A.	1	F3		

PennDOT Data (if applicable) Accident Number _____ ☐ Interstate ☐ Safety Zone ☐ Work Zone

Statute Description (include the name of statute or ordinance): **CRIMINAL USE OF A COMMUNICATION FACILITY**

Acts of the accused associated with this Offense: In that the Defendant used a communication facility to commit, cause, or facilitate the commission or the attempt thereof of any crime which constitutes a felony under Title 18 or under the Controlled Substance, Drug, Device and Cosmetic Act. TO WIT: Tyreese Lewis and co-conspirators used electronic communications to solicit and obtain personal identifying information of individuals for the purpose of exchanging personal identifying information and conduct fraudulent transfer of funds from financial accounts through online banking apps and peer-to-peer applications.

POLICE CRIMINAL COMPLAINT

Docket Number:	Date Filed:	OTN/LiveScan Number	Complaint/Incident Number
CR-319-23	7/20/23	R515432-1	FCC-22-0014

Defendant Name:	First:	Middle:	Last:
	TYREESE	L.	LEWIS

2. I ask that a warrant of arrest or a summons be issued and that the defendant be required to answer the charges I have made.

3. I verify that the facts set forth in this complaint are true and correct to the best of my knowledge or information and belief. This verification is made subject to the penalties of Section 4904 of the Crimes Code (18 Pa.C.S. § 4904) relating to unsworn falsification to authorities.

4. This complaint consists of the preceding page(s) numbered 1 through 2.

5. I certify that this filing complies with the provisions of the *Case Records Public Access Policy of the Unified Judicial System of Pennsylvania* that require filing confidential information and documents differently that non-confidential information and documents.

The acts committed by the accused, as listed and hereafter, were against the peace and dignity of the Commonwealth of Pennsylvania and were contrary to the Act(s) of the Assembly, or in violation of the statutes cited.
(Before a warrant of arrest can be issued, an affidavit of probable cause must be completed, sworn to before the issuing authority, and attached.)

(Date) (Year) (Signature of Affiant)

AND NOW, on this date 26th day of July 2023, I certify that the complaint has been properly completed and verified.

An affidavit of probable cause must be completed before a warrant can be issued.

12-2-05
(Magisterial District Court Number)

(Issuing Authority)

SEAL COURT OF COMMON PLEAS DAUPHIN COUNTY, PA

POLICE CRIMINAL COMPLAINT

Docket Number:	Date Filed:	OTN/LiveScan Number	Complaint/Incident Number
CR-319-23	1/20/23	R 515432-1	FCC-22-0014

Defendant Name:	First:	Middle:	Last:
	TYREESE		LEWIS

AFFIDAVIT of PROBABLE CAUSE

Special Agent Kathryn Grady of the Office of Attorney General, and Trooper Christopher Colarusso of the Pennsylvania State Police, being duly sworn according to law, depose and say:

I, Kathryn Grady, am a Special Agent employed by the Pennsylvania Office of Attorney General, Bureau of Criminal Investigation, and is empowered by law to conduct investigations and make arrests relating to white-collar crimes, theft, fraud, and other violations of Pennsylvania Law. Your Affiant currently holds the designation of "Certified Fraud Examiner" and has conducted numerous investigations involving financial crimes. Your Affiant has received training in electronic surveillance by the Pennsylvania State Police in accordance with the Pennsylvania Wiretapping and electronic Surveillance Control Act. This training resulted in the issuance of a class "A" certification, authorizing your Affiant to conduct criminal investigations using various wiretapping equipment, as authorized by Chapter 57 of the Pennsylvania Crimes Code. Your Affiant was certified to employ such techniques while conducting criminal investigations, maintaining "A" certification number A-5948. Your Affiant has been so employed since January 2018 and is currently assigned to the Financial Crime Section in Harrisburg, Pennsylvania. Based upon your Affiant's law enforcement experience and training, your Affiant is familiar with the manner in which various crimes are committed in the Commonwealth relating to public corruption, white collar crimes, illegal drugs, gangs, theft and fraud. Based upon the foregoing training and experience, your Affiant has special expertise regarding the practices of, and techniques used by, these offenders.

I, Trooper Christopher Colarusso, am a Pennsylvania State Trooper assigned to the Bureau of Criminal Investigation's Eastern Organized Crime Task Force. Your Affiant has been employed by the Pennsylvania State Police since 2002. During my tenure with PSP, Your Affiant has conducted numerous criminal investigations to include cases involving identity theft, fraud, forgery, and corrupt organizations. Your Affiant has been involved with investigations requiring the interdiction of individuals and groups engaged in organized criminal activity. Your Affiant has worked in a covert or undercover capacity and has utilized confidential informants to

gather intelligence and evidence. Your Affiant has conducted and/or participated in numerous criminal investigations involving court orders, search warrants and arrest warrants. During my tenure with the Pennsylvania State Police, Your Affiant has received specific training in financial and computer crimes investigations and the techniques utilized by suspects to conceal their activities from detection by law enforcement. Your Affiant has attended and completed the following training courses related to investigations involving seizing evidence from Internet Service Providers and companies that provide internet and communication services: Cellebrite UFED Field Operator – November, 2018; Cyber & Fraud Investigations – November, 2018; Dark Web / Bitcoin Investigations – January, 2018; ICAC Advanced Undercover Chat Training – October, 2016; Internet Crime Investigation – May, 2010.

I. INVESTIGATION

On September 15, 2022, your Affiants became aware of several subjects conducting similar activity involving the purchase of Visa Gift Cards within Cumberland, Dauphin, Lancaster, and York Counties. As a result of the investigation, your Affiants have identified incidents, discussed in detail below, as being related to each other and suspect the subjects are using fraudulent identities to steal debit/credit card numbers and use these account numbers to make fraudulent purchases. Through the course of the investigation, your Affiants identified various fraud incidents, which included a large-scale customer impersonation scheme involving multiple financial institutions. Your Affiants identified evidence that shows these suspects were conspiring together in a Corrupt Organization to commit the crimes of Identity Theft, Access Device Fraud, Money Laundering, Theft, and Criminal Conspiracy.

The suspects at times impersonated the employees of financial institutions to gain access to multiple bank accounts. Throughout this scheme, the suspects have stolen approximately $1.8 million from victim account holders at these financial institutions, discussed in more detail below. This table identifies the individuals involved in the ongoing fraud scheme:

Name	Theft	Access Device Fraud	Identity Theft	Bank Customer Impersonation	Unlawful Proceeds
Tyreese Lewis	X	X	X	X	X
Carl Gonzalez	X	X	X	X	X
Kristopher Davis	X	X			X
Jaire Cotton	X	X	X	X	X
Zyaire Monserrat	X	X	X	X	X
Eric Greenawalt	X	X	X		X
Corey Gray	X	X			
Derek Jones	X	X	X		
Tanayia Gotshall	X	X			X
Ricky Cruz	X	X			X
Robert Rodriguez	X	X			X
Lavon Whitaker	X	X	X	X	X
Cyrai Tillman	X	X			

II. CREDIT/DEBIT CARD AND GIFT CARD SCHEME

A. Millcreek Police Department

On September 7, 2022, Millcreek Police Department (Erie, PA) contacted Trooper Colarusso about similar, suspicious activity occurring in Dauphin County. Millcreek Police received a report from Susan Kerr related to fraudulent debit card transactions that occurred on August 19, 2022. Your Affiants reviewed the list of fraudulent transactions provided by Millcreek Police Department and determined there were 14 fraudulent transactions, which totaled $1,769.53. The transactions occurred at Giant, Rite Aid, Rutter's, Sheetz, and the Piercing Pagoda in Harrisburg, PA and the surrounding areas. The transactions that occurred at Giant, Rite Aid, Rutter's, and Sheetz were for Visa Gift Cards ranging from $25 to $400. The surveillance video provided by Giant showed the suspects, who were identified as Tyreese Lewis and Derek Jones, were driving in a white Chevrolet sedan. A third unidentified suspect was with the individuals while in the store, but drove separate in a black Chevrolet sedan. The video surveillance provided by Sheetz identified Lewis and Jones conducting the transactions while occupying a white

Chevrolet sedan. Video surveillance confirmed that Lewis and Jones utilized the Apple Pay feature on their mobile devices to complete the transactions. Your Affiants know that the use of Apple Pay to make purchases creates a tokenized number to mask the true debit/credit card number being utilized to complete the transaction. The full debit/credit card numbers are tokenized in order to prevent the account from being compromised should there be a skimmer or data breach of the system.

B. Rutter's Fraud

On September 7, 2022, Rutter's Store Corporate Security received a fraud alert from InComm, the company that issued Visa Gift Cards. The alert was generated due to a larger-than-normal amount of purchases for Visa Gift Cards at multiple Rutter's locations throughout Adams, Cumberland and York Counties. A total of 14 transactions were identified on September 7, 2022 between 09:28 hours and 21:55 hours. The transactions totaled $20,099. Due to the fraud alert received by Rutter's, Corporate Security began reviewing video surveillance and determined the same three subjects, who were later identified by law enforcement as Zyaire Monserrat, Tanayia Gotshall, and Jaire Cotton, were conducting the transactions. Corporate Security identified the vehicle being utilized by the suspects as a Red Toyota RAV4 bearing PA license plate LYG-6771. The description of the suspects and the vehicle were provided to York County Dispatch in attempts to interdict the individuals.

West Manchester Township Police Department (WMTPD) ultimately located this vehicle at a Rutter's Gas Station in York County, and identified the occupants as Jaire Cotton, Zyaire Monserrat, and Tanayia Gotshall.

The Toyota RAV4 was identified as being owned by Enterprise Rentals. WMTPD determined the vehicle was rented by Brandon Hill, who identified Monserrat as his younger brother. Pursuant to a Search Warrant, WMTPD seized five mobile phone devices, three Pennsylvania Driver's Licenses (none of which belonged to the subjects), 13 Visa Gift Cards, and multiple receipts for gift card purchases from Rutter's, Dollar General and 7-Eleven.

Rutter's surveillance video revealed that on September 7, 2022, Cotton, Monserrat, and Gotshall used Apple Pay and/or Google Pay to purchase Visa Gift Cards at multiple Rutter's locations throughout Cumberland and York Counties (Your Affiants know that the use of Google Pay to make purchases, like Apple Pay, creates a tokenized number to mask the true debit/credit card number being utilized to complete the transaction. The full debit/credit card numbers are tokenized in order to prevent the account from being compromised should there be a skimmer or data breach of the system). The gift cards were valued at $500 each. Corporate Security provided transaction data related to the fraudulent activity which identified the account numbers for the Visa Gift Cards, purchased by Cotton, Monserrat, and Gotshall.

The gift cards listed were identified as part of the vehicle search by WMTPD. During the search, WMTPD located 13 Visa Gift Cards and multiple receipts for Rutter's, 7-Eleven, and Dollar General located in the Adams, Cumberland, and York County areas. Your Affiants obtained records from InComm, the issuer of the gift cards, to confirm their purchase dates, amounts, and locations. The records also provide the following transaction history and whether the cards were flagged for potential fraud. This table details the aforementioned information:

Date and Time	Business Name and Location	Card Number (VAN)	Card Amount	Fraud Flag	Located
9/7/2022 at 15:00	Stripes LLC D/B/A 7-Eleven 101 Limekiln Rd New Cumberland, PA	6058120026236756766	$500	No	Vehicle/Receipt
9/7/2022 at 15:00	Stripes LLC D/B/A 7-Eleven 101 Limekiln Rd New Cumberland, PA	6058120015116216347	$500	No	Vehicle
9/7/2022 at 15:00	Stripes LLC D/B/A 7-Eleven 101 Limekiln Rd New Cumberland, PA	6058120040726056255	$500	No	Vehicle/Receipt

9/7/2022 at 15:17	Stripes LLC D/B/A 7-Eleven 101 Limekiln Rd New Cumberland, PA	6058120030311811925	$500	No	Receipt
9/7/2022 at 18:10	Rutter's Store 64 1150 Harrisburg Pike Carlisle, PA	6058120020710086229	$500	Yes	Vehicle/Receipt
9/7/2022 at 18:10	Rutter's Store 64 1150 Harrisburg Pike Carlisle, PA	6058120013511333148	$500	Yes	Receipt
9/7/2022 at 18:10	Rutter's Store 64 1150 Harrisburg Pike Carlisle, PA	6058120039889766098	$500	Yes	Receipt
9/7/2022 at 18:56	Rutter's Store 66 1455 York Road Carlisle, PA	6058120024677310192	$500	Yes	Vehicle
9/7/2022 at 20:17	Rutter's Store 36 3050 Heidlersburg Rd York Springs, PA	6058120040000954886	$500	Yes	Vehicle/Receipt
9/7/2022 at 20:36	Rutter's Store 17 2115 East Berlin Rd East Berlin, PA	6058120027188665343	$500	Yes	Vehicle
9/7/2022 at 20:36	Rutter's Store 17 2115 East Berlin Rd East Berlin, PA	6058120019830024896	$500	Yes	Vehicle
9/7/2022 at 20:46	Dollar General 5736 Carlisle Street New Oxford, PA	6058120014867891408	$500	Yes	Vehicle
9/7/2022 at 20:46	Dollar General 5736 Carlisle Street New Oxford, PA	6058120033570711653	$500	Yes	Vehicle
9/7/2022 at 21:03	Rutter's Store 46 113 Abbottstown St East Berlin, PA	6058120032260280078	$500	Yes	Vehicle/Receipt
9/7/2022 at 21:03	Rutter's Store 46 113 Abbottstown St East Berlin, PA	6058120026544980818	$500	Yes	Receipt
9/7/2022 at 21:03	Rutter's Store 46 113 Abbottstown St East Berlin, PA	6058120027802548750	$500	Yes	Receipt
9/7/2022 at 21:45	Rutter's Store 50 420 North Main St Spring Grove, PA	6058120024817923896	$500	Yes	Vehicle/Receipt

9/7/2022 at 21:45	Rutter's Store 50 420 North Main St Spring Grove, PA	6058120024693175744	$500	Yes	Vehicle/Receipt
9/7/2022 at 21:45	Rutter's Store 50 420 North Main St Spring Grove, PA	6058120016780236033	$500	Yes	Receipt

Rutter's Corporate Security identified the purchase of 59 additional Visa Gift Cards between August 11, 2022 and September 21, 2022 at Rutter's locations in Cumberland and York Counties. The gift cards totaled $24,800. A review of video surveillance was conducted and provided to your Affiants for review. In the video surveillance, your Affiants identified Lewis as having completed gift card purchases. In additional video surveillance, Monserrat and Cotton can be seen purchasing gift cards together at multiple Rutter's locations. In four of the transactions, which totaled $2,400, the sales were cancelled due to the card payments being declined at the point of sale. The identified suspects were using Apple and/or Google Pay to purchase the gift cards.

C. Framingham Police Department

On September 27, 2022, Your Affiants became aware of an investigation initiated in Framingham, Massachusetts once again involving Cotton, Monserrat, and Gotshall. Framingham Police contacted Rutter's Corporate Security because they were investigating a case in which a victim's credit card was utilized at various locations throughout South Central PA from August 8, 2022, through August 11, 2022. The unauthorized card activity occurred primarily in Dauphin County, but also in Cumberland and York counties. When Rutter's reviewed video footage from those dates, they recognized Cotton, Monserrat, and Gotshall as the same three people who had purchased Visa Gift Cards in bulk on September 7, 2022.

The victim, Krystal Miller, reported to Framingham Police that a subject called her from telephone number 717-869-9207 pretending to be her bank. Miller fell for the scam and proceeded to provide her name, the last four digits of her debit card number, and other personal identifying information (PII) to the caller. According to open

source records, 717-869-9207 is a T-MOBILE number associated with Zyaire Monserrat. After Miller provided her PII to the caller, she received a text message with a link to resolve the fraudulent activity. Shortly after opening this link, she then received a security message from Google that a new device had accessed her Gmail account. The security message informed her that an Apple iPhone 12 labeled "Zyairw's phone" (sic) was the device accessing her account. The scammer changed the password to her Google account, as well as the telephone number linked to her bank account.

Once your Affiant learned about the Framingham Police investigation, the transaction and surveillance records were obtained related to the fraudulent purchases made with Miller's debit card number. This information revealed that Miller's card was used to purchase Visa Gift Cards, perfume, sneakers, and other miscellaneous items at various businesses in the Greater Harrisburg area, including Speedway, Rite Aid, Dollar Tree, Dollar General, Joe's Kwik Marts, Sunoco, and Rutter's. The surveillance video obtained by your Affiants from the identified transactions depicted Monserrat and Lavon Whitaker as conducting the transactions utilizing Miller's debit card number.

D. Hampden Township Police Department

On October 7, 2023, Trooper Colarusso was contacted by Hampden Township Police Department related to fraudulent transactions that occurred at the Exxon Gas Station located at 4175 Carlisle Pike, Mechanicsburg, PA on August 10, 2022. Exxon Gas Station was able to provide video surveillance, which shows a black male attempting to purchase multiple Visa Gift cards utilizing Apple Pay on their cell phone. The individual was able to purchase eight (8) $200 Visa Gift Cards. After activating the fourth Visa Gift Card, the Exxon employee requested to verify their identity to the card processing company via telephone to activate the remaining cards. Detective David Oaster, Hampden Township Police Department, identified the debit card used to make the purchase was issued by Stanford Federal Credit Union, but was unable to obtain any customer information. The individual in the surveillance video was identified as Zyaire Monserrat.

E. Seven Hills Police Department

On October 31, 2022, Trooper Colarusso received information from Seven Hills Police Department (Seven Hills, Ohio) concerning fraudulent debit card purchases that occurred in the Harrisburg area. The Seven Hills victim, Marinel Irodia, had multiple Citizens Bank Accounts that showed unauthorized transactions had occurred at various stores in the Harrisburg area, including Dollar General and Rite Aid locations. Your Affiant spoke with Citizens Bank Corporate Security and confirmed this activity was reported as fraudulent. Your Affiants obtained video surveillance, which identified Lavon Whitaker as the individual using the victim's debit card.

F. Dollar General – West Earl Township Police Department

Trooper Colarusso made contact with Dollar General Corporate Security regarding fraudulent transactions that occurred on August 11, 2022, and on October 19, 2022. Trooper Colarusso requested video surveillance and transaction information for the suspected fraudulent purchases, and advised Corporate Security to reach out to him directly in real-time should they suspect that another fraudulent transaction is occurring at one of their locations.

On November 1, 2022, at approximately 1900hrs, Dollar General Corporate Security contacted Trooper Colarusso regarding an incident involving the bulk purchase of Visa Gift Cards that was occurring at Dollar General locations throughout Lancaster County. Surveillance video revealed that the subject was a black male driving a black SUV, whom appeared to be Monserrat. West Earl Township Police Department conducted a traffic stop in front of the Dollar General located on the 500 block of S. 7th Street in Ephrata, PA. The suspect SUV was a black Mitsubishi Outlander Sport with PA Registration LML 7247, and the vehicle occupants were identified as Zyaire Monserrat, Corey Gray, Jr., and Tyreese Lewis. Monserrat was in the rear passenger seat of the vehicle and matched the surveillance photos provided by Dollar General as the subject making the purchases. Multiple cell phones and a large quantity of gift cards were located on the rear passenger seat of the vehicle. Police seized the three cell phones

and 12 Visa Gift Cards located in the backseat next to Monserrat. Lewis and Gray denied going to any other Dollar Generals in the area and stated that they were on their way to a Philadelphia casino. Lewis told police Monserrat was using the gift cards to pay for hotel rooms and AirBNBs. The victim was identified as Sandra Campbell of Albion, Michigan. Campbell confirmed her Citizens Bank debit card was compromised and she did not authorize the purchases. Lewis also indicated he had one of Monserrat's phones, and Monserrat did in fact confirm that the cell phone was his. The items were in plain view (three cell phones and Visa Gift Cards) and were seized as evidence that pertains to this ongoing investigation.

G. Lower Paxton Township Police

On November 1, 2022, Lower Paxton Police Department became involved with an incident at Citizens Bank located at 4271 Union Deposit Road, Harrisburg, PA 17109. Jaire Cotton attempted to cash a forged check drawn on the Citizens Bank account for victim Alan Saluti of Somerville, MA. The bank teller observed the signature did not match what was on record at Citizens Bank. Officer Barber was also notified that Saluti's debit card was used for transactions at a Rite Aid and Dollar Tree in Harrisburg, PA. Officer Shayne Barber was able to confirm with the victim that Cotton did not have his authorization to cash any checks drawn from his Citizens Bank account.

On November 2, 2022, a Citizens Bank employee notified Officer Barber that they located 11 checks in the parking lot after the incident on November 1, 2022 involving Cotton. There were five (5) checks drawn on the account of Saluti and six (6) checks drawn on the account of John and Dorothy Deremer of North Smithfield, RI. Officer Barber made contact with Dorothy Deremer, who confirmed Cotton was not authorized and informed him there had been $9,800 fraudulently withdrawn from her Citizens Bank savings account.

H. Lancaster City Police Department

Docket Number:	Date Filed:	OTN/LiveScan Number	Complaint/Incident Number
CR-315-23	07/26/23	R515432-1	FCC-22-0014

Defendant Name:	First:	Middle:	Last:
	TYREESE		LEWIS

On November 14, 2022, an employee at The Heat Check located inside the Park City Mall, Lancaster, PA, reported the use of five (5) fraudulent credit cards to purchase approximately $3,700 worth of items between October 26, 2023 and October 30, 2023. The owner of The Heat Check provided video surveillance, which identified three individuals conducting the transactions. Detective Willard Smith was able to identify two of the individuals as Tyreese Lewis and Zyaire Monserrat. During the transactions, the individuals had to manually enter the debit card numbers into the Point of Sale system utilized by the business. The transactions were identified as follows:

1. 10/26/22 at 1800 hours - $750 – Tyreese Lewis and Zyaire Monserrat were identified in the video surveillance. The debit card number was not able to be identified.
2. 10/28/22 at 1605 hours - $590 – Lewis and Monserrat were identified in the video surveillance. The debit card number used was identified as Bank of America ending in 3895.
3. 10/28/22 at 1609 hours - $425 – Lewis and Monserrat were identified in the video surveillance. The debit card number used was identified as Bank of America ending in 6966.
4. 10/30/22 at 1704 hours - $685 – Lewis, Monserrat, and an unidentified suspect were observed the video surveillance. The debit card number used was identified as Bank of America ending in 4641.
5. 10/30/22 at 1717 hours - $700 – Lewis, Monserrat, and an unidentified suspect were observed in the video surveillance. The debit card number used was identified as Bank of America ending in 8145.

I. Penbrook Police Department

On November 25, 2022, Officer Brant Maley of the Penbrook Police Department in Dauphin County conducted a traffic stop on a white Audi operated by Tyreese Lewis. Pursuant to the traffic stop, a Search Warrant was obtained and executed on the white Audi. Officer Maley observed a Visa Gift Card, cash, and what appeared to be a Citizens Bank money envelope in plain view of the vehicle. Officer Maley was aware of the ongoing fraud investigation and notified your Affiants.

The vehicle search yielded seven additional mobile devices, Vanilla Visa Gift Cards, receipts from the aforementioned retail establishment The Heat Check and clothing. The Citizen Bank checkbook located inside of the vehicle was for bank customer Laurie Brantigan of Troy, New York. Your Affiants later spoke with Brantigan who confirmed that she did not authorize Lewis to possess her checkbook. Brantigan also reported fraudulent activity conducted on her Citizen Bank accounts. The Heat Check receipt found during the search of the vehicle was date and time stamped October 30, 2022 at 17:07 hours. The Heat Check confirmed this transaction was also fraud.

Your Affiants seized the seven mobile devices and Vanilla Visa Gift cards as part of the vehicle search, and then obtained a Search Warrant to retrieve the content of all ten mobile devices seized during the course of this incident.

III. Vanilla Visa Gift Cards

Your Affiant obtained records from InComm, the issuing company, related to the identified Vanilla Visa Gift Cards from the prior police incidents. The gift cards were identified as the result of seizures during the aforementioned police incidents and images found on the seized mobile devices. Your Affiants reviewed the records provided by InComm, which revealed they were purchased in the South Central Pennsylvania area. The funds were removed from the gift cards via attempted Cash App transfers, Fan Duel, Dollar Tree, Sunoco, 7-Eleven, Giant, Wawa, Door Dash, Wal-Mart, GTL Collect Calls, Sheetz, and Rutter's.

On December 22, 2022, additional images of Vanilla Visa Gift Cards, with account numbers, were discovered on mobile devices seized on November 25, 2022 from Lewis. The identified gift cards were purchased at Speedways, Dollar Generals, and Rite Aids in the Harrisburg area. The cards were used for purchases at Uber, Junk Busterz, Dollar General, Uber Eats, Door Dash, Giant, Sunoco, 7-Eleven, Roberto's Pizza, CVS Pharmacy, Paypal transfers to Zyaire Monserrat and Shelly Dent, T-Mobile, and Wal-Mart.

The gift card purchases conducted by Lewis, Cotton, Monseratt, Gotshall, Jones, and Whitaker follow a notable pattern of fraud. Specifically, the subjects simultaneously purchased multiple gift cards between $50 and $500 and traveled to multiple locations in attempt to avoid detection by the businesses. The date range of the gift card purchases was identified as January 17, 2022 through October 14, 2022. Your Affiants confirmed many of these purchases to be fraudulent.

IV. Mobile Device Analysis

A. Mobile Devices seized on September 7, 2022

During the September 7, 2022 interaction with Jaire Cotton, Zyaire Monserrat, and Tanayia Gotshall, there were five (5) mobile devices seized from the vehicle by West Manchester Township Police Department. On September 26, 2022, your Affiants obtained a Search Warrant to review the contents of the mobile devices. The following telephone numbers were identified on the seized devices: 717-869-9207, 717-343-9375, 717-315-8574, and 717-943-4668. One of the mobile devices did not have an identifiable phone number. Based on the contents and subscriber information of the mobile devices, it is believed four (4) of the five (5) mobile devices were utilized by Monserrat and the fifth device was utilized by Cotton.

Your Affiants identified approximately 220 victim names that were purchased on the website Briansclub.cm. Briansclub.cm was identified by your Affiants as a website that allows the purchase of individual's personal identifying information, including but not limited to full debit card and/or credit numbers, social security numbers, pin numbers, date of birth, addresses, and maiden names. Briansclub.cm requires its customers to use cryptocurrency to purchase the identities. There were images located on the mobile devices that reflect the purchase of the data from the website, such as screenshots of individual's personal identifying information, website images for specific Bank Identification Numbers (BIN), and shared images amongst co-conspirators. Also, on the phones were images of Vanilla Visa Gift card numbers, Apple Pay transactions, and Driver's License Identifications.

One of the mobile devices, identified as "Zyairw's iPhone", had a minimum of 24 mobile banking applications, which included Members 1st Federal Credit Union, PSECU, Navy Federal Credit Union, Citi Mobile, Zelle, Varo Bank, American Express, TAB Personal Banking, VACU Mobile Banking, Capital One Mobile, Regions Mobile, First Financial Bank Texas, Chase Mobile, Wells Fargo Bank, People's Bank, Citizens Bank, PNC Bank, Ingo Money App, Commerce Bank, Credit Karma, Chime Banking, Paypal Venmo, and Cash App. In addition, Hertz Rent-A-Car and Turo applications were found on the device, as well as on the other seized phones. Also located on the devices were screenshots from the website Fastpeoplesearch.com that matched the identities purchased on Briansclub.cm. These searches indicated the suspects were attempting to verify the information provided by the Briansclub.com purchases before attempting to call the potential victims. The screenshots also included online banking login information for Citizens Bank. In addition, the mobile device contained the personal identifying information for the Framingham victim, Krystal Miller, which was purchased from Briansclub.cm. Miller reported approximately $30,000 in fraudulent debit card transactions on her Citizens Bank account.

On the mobile device identified as utilizing phone number 717-943-4668 and being owned by Monserrat, your Affiants discovered multiple videos and images taken while he and friends were in Ocean City, Maryland. In the video, your Affiants identified Monserrat, Cotton, Lavon Whitaker, and Carl Gonzalez.

B. Mobile Devices Seized on November 1, 2022.

On November 1, 2022, West Earl Township Police Department seized three mobile devices during a traffic stop related to fraudulent Visa Gift Card purchases at Dollar General Stores in the Lancaster area. On November 7, 2022, your Affiants obtained a Search Warrant for the contents of the mobile devices. The devices were identified as being owned by Monserrat and being assigned telephone numbers 401-626-7641, 401-428-0079, and 717-943-4668. Mobile telephone number 717-943-4668 was previously identified as part of the WMTPD seizures.

In a review of the mobile devices, your Affiants identified 525 of images related to the investigation including Citizen Bank online banking usernames, debit cards, Visa Gift Cards, screenshots of Briansclub.cm, Bank of America online banking, State Driver License images, cards on Apple Wallets, Apple Pay transactions and screenshots of phone call records for individuals in with Massachusetts, Connecticut, Arizona, New York, and Michigan area codes. Based on the investigation, these phone numbers are believed to belong to victims of identity theft and vishing phone calls by the suspects. For example, a screenshot of an email from Citizens Bank online fraud detection was identified for customer, William Macfarlane. The email address identified in the screenshot was jwet1500@icloud.com. This was identified as the Apple ID on the mobile device assigned telephone number 401-428-0079 owned by Monserrat.

On the mobile device with telephone number 717-943-4668, your Affiants identified a large amount of images related to identity theft, access device fraud, and check fraud. One of the images contained a Citizens Bank bill payment check for Kirsten Klanian of Middletown, RI with account number 6320816299 for the amount of $2,487. The check was made payable to Devon James, 1070 Lakewood Dr, Harrisburg, PA 17109. Your Affiants confirmed with Citizens Bank there was fraudulent activity reported on the account of Klanian. The images also identified Monserrat's Cash App account as '$getracks17'. Monserrat used FastPeopleSearch (fastpeoplesearch.com) to look up individual's names, address, and telephone numbers. Based on the investigation conducted by your Affiants, the suspects purchased the identities on Briansclub.cm and used the FastPeopleSearch website to confirm the information was correct before making vishing phone calls to victims. A screenshot was found on this device to order checks for the Citizens Bank account in the name of Khalil Jordan. The checks were sent to 223 Francis L Cadden Pkwy Apt 101, Harrisburg, PA 17111. Your Affiants identified this address as a known residence for Jaire Cotton.

C. Mobile Devices Seized on November 25, 2022

On November 25, 2022, your Affiant seized 10 mobile devices as a result of a traffic stop in Penbrook, PA involving Tyreese Lewis. On December 6, 2022, your Affiant obtained a Search Warrant for the contents of the mobile devices. Your Affiants know from training and experience that suspects involved in fraud schemes will utilizing multiple mobile devices to conduct their activity to make it more difficult to track and identify their activity. A review of the mobile devices identified telephone numbers 201-893-1876, 717-379-1306, 717-585-1010, 717-379-6782, 267-816-4327, 717-809-9202, 412-929-2431, and 717-215-8074.

Upon review of the 10 mobile devices, your Affiants identified a large amount of images and videos that containing identifying information, debit card numbers, online banking user names, Apple Pay transactions, Apple Wallet debit cards, and other information related to this fraud investigation. The devices identified victims of Identity Theft and Access Device fraud at financial institutions including Citizens Bank, PNC Bank, Bank of America, Truist Bank, and Members 1st Federal Credit Union.

One mobile device identified by telephone number 717-379-1306 was identified as being owned by Tyreese Lewis based on the messages, images, and other data recovered on the device. The device identified social media accounts for Tyreese Lewis and messages containing the exchange of debit/credit cards numbers to other unidentified individuals. Lewis confirmed in the social media messages that his telephone number at the time was 717-379-1306. In addition, there were a large number of Google searches located on the device, which included the identification of financial institutions, scam scripts to scare, FBI agent investigating fraud, credit card companies, central debit card bin, weird spam texts, what credit card send alert through email to confirm transactions, weird spam texts to scare someone, and briansclub.cm. Your Affiant identified text messages on the device between Lewis and Monserrat (717-943-4668) related to the writing of checks to be cashed, what the split would be from the profits, and the exchange of financial banking records. A text chain was identified between Lewis and Citizens Bank in

which he was impersonating customers Leonard Goldsmith and Laurie Brantigan. Lewis was seeking to increase the ATM limits for the accounts. Citizens Bank declined to increase the daily limits. The device had approximately 500 images related to the identities of individuals, debit/credit card numbers, bank account numbers, check images, check orders, cryptocurrency transactions, firearms, and the sale of controlled substances. The device had the Telegram application and messages were able to be recovered. The recovered Telegram messages related to "The School of Jwet". The Telegram application is an encrypted program that allows users to exchange files, images, and videos within the application. The application does not require any identification be provided to register an account. Your Affiants are also aware that the term 'jwet' is utilized by scammers to identify the financial scams involving Identity Theft, Forgery, Check Fraud, and Access Device Frauds.

On mobile device identified by telephone number 717-215-8074, your Affiants identified approximately 400 images that contain personal identifying information, debit/credit card numbers, screenshots from Briansclub.cm, controlled substances, Lewis holding large amounts of cash, Visa Gift Cards, and copies of State Driver's Licenses. In addition, Google search terms were identified on the device which included multiple financial institutions, what is a cpn, my life, tyreese lewis warrant fraud, Brians Club group Chat 2022, and Brians Club hack. An additional 80 videos were identified with Lewis in the videos displaying large amounts of cash, Visa Gift Cards, merchandise, and sharing personal identifying information.

V. Members 1st Federal Credit Union Customer Impersonation Fraud

Your Affiants reviewed the identities recovered from the mobile devices seized as part of the ongoing investigation. Within the data, your Affiants identified victim, Jason Seibert. The targets of the investigation obtained Seibert's American Express and Members 1st Federal Credit Union (MFFCU) account numbers. Your Affiants made contact with MFFCU on March 23, 2023 related to the ongoing investigation. Your Affiants spoke with Corporate Security investigators related to the identified victim, Seibert. As result of the inquiry,

MFFCU Corporate Security shared they were investigating a large scale fraud involving the impersonation of MFFCU Fraud Department to victim customers via vishing telephone calls. Vishing is the use of fraudulent phone calls to trick individuals into revealing personal identifying information.

In January 2023, MFFCU Corporate Security identified multiple victims who had received suspicious phone calls from individuals claiming to be the MFFCU Fraud Department. The victims reported being asked to provide their personal identifying information, online banking sign on and password, debit card number, and to provide the two factor identification code being sent while on the phone with the impersonators. The victims would then be locked out of their accounts. The impersonators would transfer large dollar amounts out of the victim account into another MFFCU account. Your Affiants identified these secondary accounts as funnel accounts. Once the funds were transferred into the funnel accounts, the funds would be withdrawn at MFFCU branches, ATM withdrawals, cash advance transactions, or through peer-to-peer financial transaction mobile apps such as Zelle or Cash App. In this investigation, a funnel account serves as an intermediary between the victim and the suspects in order to conceal the source of the fraudulent funds. The MFFCU branches and ATMs were located in Cumberland, Dauphin, York, and Lancaster counties. The cash advance transactions were being conducted at Hollywood Casino located in Grantville, PA and York, PA.

MFFCU collected information from victims related to the vishing phone calls they received and identified approximately 30 phone numbers that made initial contact with the customers. Based on your Affiants' investigation, it appears multiple telephone numbers were spoofed to make it appear as though the caller was a Members 1st Federal Credit Union employee and matched what would be found on the victim's debit card or if a Google search for the bank's phone number was conducted. Spoofing is when a caller deliberately falsifies the information transmitted to your caller ID display to disguise their identity. Your Affiants identified several phone numbers linked to Lewis that were identified by MFFCU vishing victims. The identified telephone numbers are

717-943-4208, 223-269-3859, 717-602-3741 717-421-8450, 717-908-7176, and 717-307-7472. Lewis provided these numbers as his point of contact via social media messages with other co-conspirators involved in the fraud scheme. In addition, your Affiant identified telephone number 775-430-6123 for Lewis through the use of legal service. This telephone number was identified by seven (7) vishing victims at MFFCU.

MFFCU provided your Affiants with video surveillance from the identified fraud transactions, which include images of subjects withdrawing cash at locations in Cumberland, Dauphin, York, and Lancaster counties. The surveillance video also included vehicles identified as involved in the transactions.

Your Affiants interviewed multiple subjects that opened or had existing accounts with Members 1st Federal Credit Union in order to receive funds stolen from vishing victims. The accounts that received the stolen funds were identified as funnel accounts. Once the funnel accounts received deposits, the stolen funds were withdrawn via cash withdrawals, point of sale transactions, or peer to peer transfers.

1. On April 19, 2023, your Affiants interviewed Witness #1, who identified Ricky Cruz as the individual who recruited them through Instagram to make $2,000 by helping him move some money through their account. Witness #1 identified Cruz's Instagram account as 'sb4slick'. Witness #1 explained Cruz asked then to open a MFFCU account in order for him to deposit money since he was unable to open an account. Cruz met Witness #1 at Sheetz near Willow Street, Lancaster, PA and drove them to the MFFCU branch across the street. Cruz instructed Witness #1 to withdrawal $10,000 in cash and keep $2,000 for themselves. Witness #1 withdrew the remaining $2,000 from the account at MFFCU located on Greenfield Road, Lancaster, PA and met Cruz at a local barber shop to provide him with the money. A review of surveillance video provided by MFFCU related to the Willow Street cash withdrawal showed a dark colored Nissan displaying PA registration LWW2407. Your Affiants determined this vehicle was registered to Ricky Cruz. Witness #1 provided text messages with Cruz to corroborate this statement.

2. On April 27, 2023, your Affiants interviewed funnel account owner, Witness #2. Witness #2 stated they had liked a Facebook post about grant money available for MFFCU account owners with the phrase "YC Tap In". Witness #2 believed the Facebook account could be identified as "Top Notch Da Don". Witness #2 personally knows the suspect, but does not know his real name. The suspect identified by Witness #2, instructed him to open the MFFCU account, provide the account number, online banking login and password, debit card number, and PIN number. Witness #2 was instructed to withdrawal funds at the MFFCU ATM located on Whiteford Road, York, PA, the Hollywood Casino located in York, PA, and then "Top Notch Da Don" used Witness #2's debit card at the Wal-Mart located in East York, PA. Video surveillance was provided by MFFCU related to the ATM transactions. Witness #2 was observed at the ATM transaction, then the suspect pulled up behind him and removed the receipt from the ATM. Video surveillance from the ATM withdrawal identified the vehicle as a dark Honda sedan with PA registration LZD8543. Witness #2 and the suspect also went to Wal-Mart in East York, PA to withdrawal funds from the funnel account. Video surveillance was obtained and corroborated the description provided by Witness # 2 of a black male wearing a neon safety vest and hat. The suspect known as "Top Notch Da Don" was later identified by your Affiants as Kristopher Davis.

3. On May 4, 2023, your Affiants interviewed Witness #3. Witness #3 stated they were recruited through the Instagram account identified as 'robinjwett'. Witness #3 stated they know the individual as Carl, but did not know his last name. Witness #3 knows Carl through their cousin, who goes to school at Central Dauphin East High School in Harrisburg, PA. The initial contact with Carl was through Instagram, but then moved to the Telegram app. Carl identified his account on Telegram as "@mrotpbott". Carl also identified his telephone number as 215-888-9956. Carl stated he was seeking persons with MFFCU accounts and told Witness #3 they could earn $5,000. Witness #3 provided your Affiants with screenshots from the Telegram

conversation and the text message chain with Carl. Witness #3 stated they met Carl at a Rutter's to provide him their debit card to complete the transaction. Your Affiants later identified Carl as Carl Gonzalez of Highspire, PA. Carl instructed Witness #3 to link their MFFCU debit card to Cash APP for the transfer of funds to Cash App account "$Murphy3xxx". Your Affiants showed Witness #3 a photo lineup and they identified Carl Gonzalez as the individual they communicated with and met at a Rutter's Gas Station in York, PA to provide their debit card.

4. On May 10, 2023, Trooper Colarusso interviewed Witness #4. Witness #4 stated he observed a story or post on the Instagram account of Robert "Macho" Rodriguez. The Instagram account was identified as 'mach.faded'. The post was soliciting the use of Members 1st bank accounts in exchange for money. The two discussed the use of the bank account through direct message on Instagram. Witness #4 provided their online banking username and password to Rodriguez. Witness #4 received a deposit into their account and was provided instructions by Rodriguez to withdrawal the funds, which they did at the MFFCU branch on Whiteford Road, York, PA. Witness #4 withdrew the funds and then met Rodriguez at a nearby Rutter's gas station to provide the money. Witness #4 only received $20 of the cash, which Rodriguez indicated was for gas.

5. On May 11, 2023, Trooper Colarusso interviewed Witness #5. Witness #5 stated they observed a story or post on the Instagram account of Eric Greenawalt. The Instagram account was identified as 'eb00k9'. The post was soliciting the use of MFFCU accounts in exchange for money. Witness #5 was able to provide Trooper Colarusso with screenshots from the Instagram direct messages between them and Greenawalt. Witness #5 was instructed by Greenawalt to withdrawal the funds that were deposited into their MFFCU bank account. Witness #5 stated they witnessed Greenawalt communicating with an unknown person via text message and phone calls during the time of the transactions. The unknown person was providing

Greenawalt instructions on when to withdrawal the funds from the account. Witness #5 was given $2,500 for the use of their bank account. Witness #5 identified Greenawalt's telephone number as 717-406-2541.

6. On June 14, 2023, your Affiants interviewed Witness #6. Witness #6 stated they were contacted through Instagram user 'robinjwett'. Witness #6 was able to identify this individual as Carl, with an unknown last name, as an individual that they previously attended school with at Central Dauphin East High School in Harrisburg, PA. Your Affiants previously identified Instagram user 'robinjwett' as Carl Gonzalez. Witness #6 provided screenshots of the messages between them, which provided information related to Witness #6's MFFCU account and the verification that the debit card was linked to a Cash App account. Witness #6 stated Gonzalez picked them up at their home and drove to the MFFCU Derry Street branch to withdraw the funds that were deposited into the account. Witness #6 withdrew $420 from the account and was able to keep $250. The account received an additional $2,000, which was then transferred via Cash App. Witness #6 stated that there was another individual in the vehicle who sat in the front passenger seat. Witness #6 was located in the rear passenger seat. While in the vehicle, Gonzalez was on Facetime with an individual who Witness #6 recognized as someone that also attended school at Central Dauphin East High School. Gonzalez was discussing with the individual on the Facetime call how to move the money into and then out of the MFFCU account owned by Witness #6. Witness #6 indicated the caller wanted their social security number, but they refused to provide that information. Witness #6 was able to see the phone clearly because of their positioning in the vehicle. Witness #6 could not recall the individual's name. Witness #6 agreed to review two photo line ups with potential suspects. Witness #6 identified Gonzalez in the first photo lineup as the individual that took him/her to the Derry Street branch. During the second photo lineup shown to Witness #6, he/she identified Tyreese Lewis, who they recognized as being on Facetime with Gonzalez while in the vehicle.

7. On July 13, 2023, your Affiant interviewed Witness #7 who had an account at MFFCU. Witness #7 received approximately $10,000 in to their account. The funds were moved as follows: $4,000 of the funds were transferred to a third MFFCU account; $1,000 to their Cash App account; and $5,000 was withdrawn in cash at the MFFCU Derry Street, Harrisburg, PA location. Witness #7 indicated Lavon Whitaker recruited them to use their MFFCU account. Witness #7 was skeptical at first that this was a scam, but was assured there were no checks going into the account and they would not get in trouble. Witness #7 received $1,000 from the transaction. Witness #7 stated Whitaker picked up the cash after the withdrawal occurred. Witness #7 also implicated Zyaire Monserrat as being involved in the fraud scheme. Witness #7 said $1,000 was sent to their Cash App account from MFFCU and then they had to transfer the money to Monserrat. Witness #7 was able to provide a screenshot of the transaction from their Cash App account. Witness #7 indicated Whitaker and Monserrat utilize their social media accounts to seek bank accounts and instruct individuals to "Tap In". Witness #7 identified Whitaker's social media account as 'Von DaDon' on Facebook and Monserrat's Snap Chat identifier as 'zy-money1018'.

As of July 14, 2023, MFFCU has identified 342 vishing victims and approximately 449 funnel accounts, which the fraudulent funds were transferred. Once the funds were moved to the funnel accounts, they were withdrawn via cash or through peer-to-peer transfers. In some instances, the funds were transferred into a secondary funnel account. The total funds transferred from the vishing victim accounts is $1,669,641.39. MFFCU Security Department was able to prevent additional loss and recover a portion of funds for the victims. The loss to MFFCU is currently $1,154,064.18.

VI. Social Media Content

Based on the training and experience of your Affiants, it is known that fraud scammers will often utilize social media platforms to recruit and promote their fraud schemes. The social media accounts for Tyreese Lewis, Jaire

Cotton, Zyaire Monserrat, Tanayia Gotshall, Carl Gonzalez, Eric Greenawalt, Robert Rodriguez, and Kristopher Davis were identified through the investigation by witness statements and open source searches. Your Affiants monitored these social media accounts and identified posts and/or stories that promoted the need for bank accounts at multiple financial institutions, which included Citizens Bank, Members 1st Federal Credit Union, PSECU, PNC Bank, Bank of America, and multiple others. Terminology such as "tap in" was used on the posts, which indicates the follower should contact the user directly if they have an account or multiple accounts to be used. The follower may or may not be aware that they are participating in a scam during the initial contact. As a result of the social media posts and witness statements, your Affiants obtained Search Warrants seeking social media content for the identified suspects.

A. Social Media Accounts of Tyreese Lewis

The Facebook and Instagram accounts of Tyreese Lewis were identified as the user name 'Heavyy Homiee'. Within the direct messages of Lewis's social media accounts, your Affiants discovered numerous messages pertaining to the recruitment of individuals for the use of their bank accounts or to assist in recruiting others in exchange for a split of the profits. Specifically, Lewis had conversations with the social media accounts of Carl Gonzalez, identified as Facebook account 'Carl Gz', Tyrone Miller identified as Facebook account 'Da Bol Philly', Jaire Cotton identified as Facebook account 'Jay Dunnie', Kristopher Davis identified as Facebook user 'Sino Topshelf Torrio' and Instagram account 'capitolboyhavinn', Shahid ElshaBazz identified as Malik Shahid Defrietas, Lavon Whitaker identified as Facebook account 'Von DaDon', and Erik Santos Greenawalt identified as Instagram user 'eb00k9'. The messages with these individuals specifically reference Members 1st accounts that were identified as having been hacked and/or agreed to open or use an existing MFFCU account to receiving fraudulent funds and split the profits with Lewis.

In multiple direct messages identified on the Facebook and Instagram accounts of Lewis, he identified multiple telephone numbers in which the persons he was communicating with could contact him. The telephone numbers were identified as 717-903-9272, 717-943-4208, 717-307-7472, 223-269-3859, 717-602-3741, 717-608-4678, and 717-908-7176. These telephone numbers were identified previously in this Affidavit based on information provided by Members 1st Federal Credit Union related to the vishing phone calls. Your Affiants attempted to identify the subscriber information for the telephone numbers. Unfortunately, they were all pre-paid phones which did not require any identification at the time of purchase to activate the devices.

In the messages, several, but not all, Members 1st Federal Credit Union funnel and victim accounts were identified. Based on the messages it appeared that individuals provided accounts to Lewis, which included online banking information. Lewis provided instructions on what to do after the funds were deposited into the funnel accounts. Tyrone Miller provided MFFCU account number 2182806923 of James Baker to Lewis. Lewis provided instructions to have Baker conduct a $3,000 cash advance at the local casino, a second withdrawal for $1,000, and then go to an ATM to withdrawal the remaining $1,000. Lewis made arrangements for Miller to meet someone at the local Wal-Mart in Harrisburg, PA to hand over the withdrawn funds. Lewis instructed Miller to forward his cut of the funds to Cash App account $JorgeCruzEspinoza1. A review of Lewis's call detail records indicate he is in communication with the telephone number associated with this Cash App account, which was identified as 562-383-8461.

According to the direct messages, Kristopher Davis sent Lewis multiple MFFCU account numbers. The accounts numbers were 1183188 for Emery, 1086459 for Hodge-Barnes, and 789676 for Skyes. Lewis provided Davis direction to send his cut of the funds to two different Cash App accounts. The accounts were identified as $JorgeCruzEspinoza1 and $jaymorgan813.

Facebook user identified as 'Bangco Bangco' provided Lewis with the MFFCU account 1188392 for Suluki. Your Affiants confirmed that the identified MFFCU accounts in the Facebook and Instagram messages were funnel accounts that received fraudulent transfers and then withdrew the funds through cash withdrawals and Cash App transfers.

In addition to the two Cash App accounts identified in the messages with Davis, Lewis provided additional Cash App names to other Facebook and Instagram users, which were identified as $murphy3xxx, $zyskudd, and $juanlomore. A screenshot was sent to Lewis, which identified a Cash App account titled "Dummy". A like-titled account was identified in fraud transactions on multiple MFFCU funnel accounts after the fraudulent transfers were completed.

Also within the messages, Lewis identified multiple Telegram accounts that he directed individuals to continue their conversations related to the sale of controlled substances and fraud activity. Those accounts were identified as EastCoastWaves, BurnWavesDown, Bubbabubjwet, and Stuff'd Puffz Exotics Menu. The accounts of EastCoastWaves, BurnWavesDown, and Stuff'd Puffz Exotics Menu were identified as channels on the Telegram account which are open to the public to follow. The account identified as Bubbabubjwet was identified as a private message account. Lewis also had these accounts linked on his Instagram page for individuals to access.

The review of Lewis's social media account also included videos and images that were loaded by the user to their Story and/or walls to recruit individuals with financial accounts at specific institutions such as Bank of America, Members First Federal Credit Union, PNC Bank, Navy Federal Credit Union, and Citizens Bank. The videos showed Lewis pulling cash from ATM machines. Lewis could be identified based on a distinct hand tattoo depicting the Mercedes Benz logo. The videos also provided links to the

multiple Telegram channels that were run by Lewis and identified as Stuff'D Puffz Exotic Menu and BurnWavesDown.

B. Social Media Accounts of Jaire Cotton

The Facebook and Instagram accounts for Jaire Cotton were identified as 'JayDunnie' on both social media platforms. Your Affiants applied for and executed search warrants on the aforementioned social media accounts. In reviewing the results, your Affiants identified direct messages between Cotton and other individuals related to Identity Theft, Access Device Fraud, and Forgery. Specifically Cotton engaged in conversations with Carl Gonzalez whose Facebook account was identified as 'Carl Gz', Tyreese Lewis whose Facebook account was identified as 'Heavyy Homiee', Kapree Wells whose Facebook account was identified as 'Swipette Tweet', Malik Shahid Defreites whose Facebook account was identified as 'Shahid ElshaBazz', Jacob Gonzalez (the brother of Carl Gonzalez) whose Facebook account was identified as 'Whitey Bulger', Christian Rodriguez whose Facebook account was identified as 'Christian Rodriguez', and Tanayia Gottshall whose Instagram account was identified as 'tanayia.aa'. The messages identified information related to the September 7, 2022 incident with West Manchester Township Police Department, Briansclub.cm activity, and fraud activity involving Members 1st and Citizens Bank.

Cotton and Gonzalez exchanged direct messages related to assistance with making vishing phone calls. Gonzalez sent Cotton screenshots related to customers at Citizens Bank, whose information was obtained through Briansclub.cm. Gonzalez asked Cotton for a phone script to start practicing the vishing phone calls. Cotton and Defreitas exchanged direct messages in which Defreitas explained he had someone with Members 1st Federal Credit Union accounts and that he could not use his because they had already blocked the account. The two were going to split $3,000 three ways. Defreitas also spoke with

Lewis in direct messages stating he had a Members 1st account. Shortly after the conversation, Defreitas received a fraudulent transfer to his account and attempted to withdrawal the funds, but MFFCU was able to prevent the withdrawals before they occurred.

Cotton and Jacob Gonzalez had a direct message conversation related to the West Manchester Township Police Department incident on September 7, 2022. Cotton wrote, "we was jwettin took 20 bands from us I was getting kiney uo da 20 ball clearin this bank and they store manager called da cops and put a be on da look out for whip dey hopped out on us at a gas station detained niggas". In your Affiants' training and experience, the term 'jwettin' is a term used for describing fraud scams.

In addition, Cotton had a direct message conversation with Christian Rodriguez. Rodriguez explained Bubba, which is a known nickname for Tyreese Lewis, deposited $4,000 into his MFFCU account and they moved it all to Cash App, but MFFCU had recently reached out to him to say his account received a fraudulent transfer. Rodriguez was concerned with what to do about the transaction and was seeking advice from Cotton. Rodriguez wrote a script of what he was going to say to the MFFCU Fraud Department related to the activity and claim his Cash App account had been hacked. Rodriguez asked Cotton what the split would be if he started to bring accounts to him instead of Lewis. MFFCU was able to confirm Rodriguez had a fraudulent transfer into his MFFCU account. Based on the transaction history it appears the fraudulent transfer was third in line in fraud transfers, which is indicative of money laundering, other MFFCU accounts prior to being deposited into Rodriguez's account. The funds were then transferred to the Cash App account of Christian Rodriguez through two transactions.

In an Instagram direct message with Tanayia Gottshall, Cotton explained that he had made contact with Lewis and that they needed to make more money to cover his court costs and bail that he had to post as a result of the September 7, 2023 gun charges. Gottshall stated Brandon [Hill] wanted money for the

vehicle rental. On the day of the WMTPD incident Gottshall, Cotton, Monserrat and Christian were in a Toyota Rav4 that had been rented by Hill. Within the conversation, Cotton identified Don Deno and Seven as willing participants as runners to conduct the fraud transactions. Law enforcement identified Seven as Cyrai Tillman, who was identified as a co-conspirator of this investigation. The two also discussed using Rite Aid and Dollar General Stores to buy gift cards and do transactions with cash back to pull the money off the cards.

The review of Cotton's social media account also included videos and images that were loaded by the user to their Story and/or walls to recruit individuals with financial accounts at specific institutions such as, but not limited to, Members First Federal Credit Union and Citizens Bank. Cotton captioned one video with, "Who can I send 5,000 to real quick that got a citizens I wanna bless you".

C. Social Media Accounts of Kristopher Davis

The social media accounts were identified for Kristopher Davis as Facebook account 'Sino Topshelf Torrio' and Instagram account 'Capitolboyhavinn'. Davis was identified in video surveillance provided by MFFCU. Your Affiants identified multiple direct messages with Davis and other individuals who exchanged information related to ongoing fraud schemes, including activity at Members 1st Federal Credit Union. Direct messages were identified between Davis and multiple targets of the fraud investigation which included Eric Greenwalt whose Instagram account was identified as 'eb00k9', Grace Sersch's Instagram account 'gracieraynn', Tyreese Lewis whose Instagram account was identified as 'Heavyy Homiee',

A direct message was identified between Davis and Instagram user 'zazascan' related to the MFFCU funnel account identified for Christopher Holmes. The user indicated that the account had been burnt.

A transfer of $7,000 had been deposited into Holmes's account. After the transfer, Holmes withdrew $1,000 at a MFFCU ATM located on Whiteford Road, York, PA.

A direct message was identified between Davis and MFFCU account owner Grace Sersch identified as Instagram user 'gracieraynn'. Sersch confirmed she had a MFFCU account, but was worried about getting in trouble. Davis instructed her to report it as fraud after they get all the money out of the account. Your Affiants learned that the funnel account owned by Sersch received a $5,000 fraudulent transfer. The funds were withdrawn through a Cash App transfer to Serschs' own account in the amount of $1,500.

A direct message between Davis and Lewis was identified which contained information related to the ongoing fraud scheme involving bank accounts. Davis inquired if Lewis had any additional accounts ready for them to work. There were additional messages found that specifically discussed the cut for each account that is brought and they are able to move money through. During the conversation, the two started an audio call and your Affiants were unable to identify the context of that conversation.

Additional messages were identified that involved the MFFCU funnel accounts for Sadiq Hawk, Felicia Diggs, Laquanda Simmons, Witness #1, Barbara Ellison, Danashia Griffin, and Witness #2. The messages contained information such as online banking logins, account numbers, debit card pin numbers, and discussions of how much the split would be for each account.

The review of Davis's social media accounts also included videos and images that were loaded by the user to their Story and/or walls to recruit individuals with financial accounts at specific institutions such as Bank of America, Members First Federal Credit Union, and Citizens Bank. Specifically, Davis posted on February 13, 2023 a video with the caption "MONEY MOVES MONDAY LETS START YOUR WEEK OFF THE RIGHT WAY! ALL ACTIVE BANKS TAP IN TO GET PAID". On February 19, 2023, Davis posted a video while outside of a Members 1st Federal Credit Union branch with the

caption "ONLY TAKING 7 SO IF YOU GOT ACTIVE MEMBERS 1ST DM ME FOR GUARANTEED FUNDS".

D. Social Media Accounts for Carl Gonzalez

The social media accounts for Carl Gonzalez were identified as Instagram accounts 'robinjwett' and 'robinjwettlogs'. After receiving the social media content for the co-conspirators of this investigation, the Facebook account for Gonzalez was identified as Carl Gz. Your Affiant was able to confirm this account is still active, but now displays the name Benjamin Franklin. Your Affiants identified multiple direct messages related to Identity Theft, Access Device Fraud, and Theft. Gonzalez was provided the account number and customer names for multiple financial institutions, which included Citizens Bank and Members 1st Federal Credit Union. In addition, Gonzalez was asked to make vishing phone calls by Instagram user 'fastrackz_spazz'. The user offered $150 per phone call. Gonzalez sent a screenshot to the user, which contained names, dates of births, and telephone numbers of multiple individuals. Gonzalez instructed the user to plug all of the information into the Citizens Bank online application.

Your Affiants identified multiple direct messages identifying MFFCU accounts. These accounts included those of Witness #3, Witness #6, Irene Montalvo, Jesse Yepes, Anthony Fox, Rayshawn Johnson, Elizabeth Hovan, Drayton Saunders, and Marcel Dawson. In the messages, an additional Cash App account of $FNharden was identified. The Instagram profile for Gonzalez also identified a Telegram channel titled "Members First". Based on your Affiant's training and experience, Telegram channels are viewable by anyone with the Telegram application, which is an end to end encrypted application.

The second identified Instagram account for Gonzalez, identified as username 'robinjwettlogs' was reviewed. It showed that Gonzalez hacked the previous account owner's Instagram page and renamed

it. The account has had several usernames since Gonzalez took it over, which include 'anonymouslogsservices' and 'Computer Geek'. Gonzalez offered the original owner to buy the page back for $50. Gonzalez also attempted to reach out to friends on the Instagram page claiming to need money because their car was stranded.

The review of Gonzalez's social media accounts also included videos and images that were loaded by the user to their Story and/or walls to recruit individuals with financial accounts at specific institutions such as Bank of America, Members First Federal Credit Union, PNC Bank, Navy Federal Credit Union, and Citizens Bank. The videos showed Gonzalez pulling cash from numerous ATM machines. For example, on May 18, 2023, Gonzalez posted an image to his Instagram Story with the caption "PSECU MEMBERS CHASE BOA REGIONS TD NAVY FED TRUIST WELLS PNC SANTANDER M&T CITIZENS FIRST NATIONAL CAP1 ALL CREDIT UNIONS Bring any of these n we can make sum money, Come Serious, an Ready to Work! Everything 10k or Better! Any bank fr". The videos and Instagram profile for Gonzalez also linked his Telegram Channel, which was identified as MembersFirst.

E. Social Media Content for Ricky Cruz

Your Affiants obtained records for social media account owned by Ricky Cruz, which was identified as Instagram account 'sb4slick'. Your Affiants identified direct messages between Cruz and Eric Greenawalt, whose Instagram handle was identified as 'eb00k9', and with Robert Rodriguez, whose Instagram handle was identified as 'mach.faded'. Greenawalt was identified by owners of MFFCU funnel accounts as having recruited them for their account information. Cruz described to multiple individuals in direct messages related to bank fraud how the scam works. Cruz explained the funds would be deposited into the account and then the cash will get pulled out at the casino depending on how much "he" drops.

F. Social Media account for Eric Greenawalt

Your Affiants obtained the social media content for Instagram account 'eb00k9' of Eric Greenawalt. Within the direct messages of the social media content, your Affiants identified conversations with Kristopher Davis whose Instagram account was identified as 'sauceboss.sino', Tyreese Lewis whose Instagram account was identified as 'heavyyhomie', Ricky Cruz whose Instagram account was identified as 'sb4slick', and Robert Rodriguez whose Instagram account was identified as 'mach.faded'. The messages contained information related to the ongoing fraud with Members 1st Federal Credit Union, as well as additional financial institutions such as Chase Bank. Greenawalt identified his telephone number as 717-844-3859.

VII. Telegram Channels

Based on the review and monitoring of social media content, your Affiants identified multiple Telegram channels related to the investigation. Telegram is a messaging app with a focus on speed and security. The messaging app is an encrypted, cloud-based and centralized instant messaging service that allows user to set up Channel, private messages, and share media files and documents. The users of Telegram can log in and out of multiple devices to access the Channel or private messages.

A. Telegram Channel BurnWavesDown

Lewis identified Telegram channel BurnWavesDown on his social media platforms and provided a link to followers to get additional information related to the fraud scheme. Your Affiants reviewed the contents of the BurnWavesDown channel which revealed the channel was created on February 25 and has 218 subscribers. It is not required to be a subscriber to review the content in the BurnWavesDown channel. The channel included images of multiple online banking accounts for Bank of America, Huntington Bank, Truist Bank, and other financial institutions. The information was listed for sale and

prices were based on the account and/or size of the potential payout. For example, on March 14, there was a post to the channel seeking bank accounts and a solicitation for bank accounts at specific financial institutions that were at least six (6) months old. The financial institutions on the list included Members First Federal Credit Union, Bank of America, Chase Bank, Citizens Bank, PNC Bank, and Truist Bank. The payouts ranged from $10,000 to $40,000.

There were images posted with multiple Apple iPhones for sale, fake state identifications, and hacks for Uber, Lyft, Door Dash, and Grubhub accounts. Lewis also posted an advertisement for lessons on how to scam starting at $250. For $1,000 Lewis stated he could teach you how to get your own logs to make money. Lewis also discussed the use of "giftcarding method" for beginners. Lewis explained that you find low security gift card stores and keep the dollar amounts low to beat the bank algorithms.

B. Telegram Channel MembersFirst

Your Affiants identified the Telegram Channel titled MembersFirst through the monitoring and review of social media content created by Carl Gonzalez. The channel was created on December 31, 2022 and currently has 234 subscribers. The contents of the channel include the sharing of customer information, which is listed for sale. Gonzalez was also offering lessons to teach the scam methods for $500. On February 8, 2023, Gonzalez posted to the channel, "If you got any Members 1st, Citizens Bank, BOA, Wells tap in guaranteed money for your. Bring me any bank and we can make some pape. Also got $ for people who are willing to go open an account. Lmk if interested". Gonzalez provided a menu of different scams he had available, which included email spams and telephone bots. Gonzalez posted images and videos which contained Citizens Bank and Members 1st Federal Credit Union account information, as well as large stacks of cash. Gonzalez also indicated he knew hacks for free Door Dash,

Uber, Lyft, and other similar services. Included in the images posted to the Channel, were identified funnel accounts, which were involved in the movement of fraudulent funds.

VIII. Cash App Analysis

Your Affiants utilized the information obtained through records provided by MFFCU, social media content, and witness information to identify the Cash App accounts of the co-conspirators of this fraud ring. Cash App is a peer to peer account transfer service owned by Block Inc. Cash App allows individuals to transfer funds between friends and family without sharing their bank account number(s). The accounts are created through the use of telephone numbers and/or email addresses. Cash App allows individuals to pick Display Names, which can mask the true identity of the account user. In addition, the accounts are identified by cash tags, which are created by the account user. Multiple debit/credit card and bank accounts can be linked to a Cash App account as a source of funding. Cash App also allows user to make cash deposits into their account at local convenient stores through a QR code generated within the application. Based on your Affiants' training and experience, Cash App is a commonly used peer to peer service utilized in fraud scams in attempt to conceal the source of the funds. The fraudsters will utilize phrases such as rent, car payment, or other generic terms in attempts to hide the reason for the funds transfer. It is also common for fraudsters to open multiple Cash App accounts with fraudulent identities to conceal the true owner and operator of the account.

Cash App accounts were identified for Zyaire Monserrat, Tanayia Gotshall, Carl Gonzalez, and Tyreese Lewis. A review of the accounts show similar transactions and recipients of funds identified as Courtney Brown, Don Deno, Lachelle, Jorge Cruz-Espinoza, Richard Lawson, Heidi Murphy, Courtney B, Robinjwetts, Juanita Larmer, and Jwet Milly.

Your Affiants identified multiple Cash App accounts for Zyaire Monserrat. The Cash App cash tags were identified as $getracks17, $getracks10, and $trnchmazzi10. Within these records, your Affiants identified six (6)

payment sources that were added or attempted to be added to the respective Cash App accounts. Specifically, the Cash App account identified as $getracks17 sent funds to Cash App accounts identified as Zy&Nay, Lachelle, Courtney Brown, Don Deno, and Abanoub K. The dollar amounts of the transfers were consistent with witness statements related to the split between them and Monseratt and/or his co-conspirators.

Tanayia Gotshall had multiple Cash App accounts identified with cash tags $tanayiagotshall, $pr3ttynayaa, and $naya3aa. The Cash App account identified with cash tag $naya3aa utilized a Display Name of Zy&nay, which had identifiable transfers with Monserrat. Gottshall had 32 payment sources added to her account and of these accounts 19 of the debit card numbers were identified from the Briansclub.cm screenshots found in Monserrat's mobile devices seized on September 7, 2022. The debit card numbers identified accounts at PNC Bank, Citizens Bank, and Members 1st Federal Credit Union. Your Affiant obtained records from PNC Bank for the debit cards that were identified on the mobile devices and confirmed there were no fraudulent transactions filed. Cash App blocked the PNC Bank accounts which were attempted to be added to Gotshall's Cash App account. Additionally, there were five (5) Citizens Bank debit cards attempted to be added to the account, but were blocked due to too many failed attempts. The MFFCU debit card for victim Jason Seibert was attempted to be added to the account, as well as their bank account number. Based on the transaction history, there were several attempts to transfer funds from the Cash App account of Seibert to Gotshall, but they were declined.

Your Affiants identified and confirmed with Seibert the Cash App account identified as $seibag1976 was not authorized to be opened using his personal identifying information. The telephone number attached to Seibert's Cash App account was listed as 717-869-9207. This telephone number was identified as being owned by Monserrat. Additional transfers were identified on Gotshall's account with Cash App users Lachelle, Zyaire Monseratt, Von Da Don, and Don Deno. Additional MFFCU funnel accounts were identified as payment sources based on the funds transfer records provided by Block Inc.

Your Affiants identified approximately 11 Cash App accounts believed to be created and operated by Tyreese Lewis. Three of these accounts were opened using Lewis's personal identifiers. These Cash App tags were identified as $timmmtable, $tinny5533, and $justvonx. The records for these accounts show there are transfer of funds that fit the pattern and dollar amount of the fraudulent activity between Lewis and Courtney B. The Cash App account identified as $justinvonx had a Citizens Bank debit card linked to one of the identity theft victims identified through Briansclub.cm screenshots on Lewis's seized mobile devices.

The other eight (8) identified Cash App accounts were identified through the telephone numbers and his social media messages. The Cash App account for cash tag $murillooy of Veronica Murillo was identified through telephone number 717-908-7176, which Lewis provided to multiple Facebook users to contact him with. In addition, a review of the account activity identified IP Address 174.251.162.190, which matches the IP history based on legal service that was initialized on Lewis' Instagram account. The account identified seven payment sources from multiple financial institutions. The account had multiple payment sources listed, which included MFFCU debit cards ending in 3236 and 1905. The MFFCU debit card ending in 3236 was identified as issued to victim Lori C Hamlin-Kopf. The transaction history showed attempts to transfer funds in $100 increments to the Cash App account of Richard Larson. The Cash Tag was identified by Lewis in social media messages in which he provided instructions to multiple individuals to transfer money to this specific account after fraudulent funds were deposit into the MFFCU funnel account.

Lewis also identified Cash App cash tag $juanlomore, which based on the records utilized telephone number 717-421-1054. The name identified on the account was Juanita Larmer. This telephone number was used to make vishing phone call to MFFCU victims. There were four MFFCU debit cards added as payment sources to this account. The identified MFFCU cards were verified to have had attempted fraudulent activity on the accounts. Your Affiants identified one debit card number to be tied to a vishing victim, who had funds transferred from their MFFCU

account fraudulently. The victim was contacted by telephone number 223-269-3859, which Lewis identified in his social media numbers as a point of contact for him. In addition, the transaction history shows movement of funds between the account and Courtney B, Abanoub K, and Richard Lawson. The cash tag was identified by Lewis in social media messages in which he provided instructions to multiple individuals to transfer money to this specific account after fraudulent funds were deposit into the MFFCU funnel account.

In the social media content obtained for Tyreese Lewis, he identified the use of Cash App account $zyskudd, which is in the name of Zyaire Green. The account had 15 payment sources added. The majority of these were blocked by Cash App due to fraud risk. In addition, similar Cash App accounts were identified to have exchanged money via Cash App such as Courtney B, Abanoub K, Heidi Murphy, and Jorge Cruz-Espinoza. The transfers ranged between $50 and $2,500.

The Cash App account with cash tag $paulykern was identified via telephone number 223-269-3859. The telephone number was identified by Lewis in his social media messages as a way for individual to contact him. This number was also identified by multiple MFFCU vishing victims. The account was initially registered using the name Tonya Cromwell, but then was changed to Augustine Madukwe. Cash App was unable to verify either of these identities. The payment source added to the account was identified as a MFFCU debit card ending in 4400. MFFCU verified this card was issued to April Cross, who reported fraud on her account. The card was closed. This card number was identified in the social media messages between Layonnie Peterson and Lewis.

Cash App cash tag $lawsonrichh was identified via social media messages in which Lewis instructed individuals to transfer funds to this account. The account was registered using the identity of Richard Lawson and telephone number 717-307-7472. The telephone number was identified by Lewis in multiple social media messages where he instructed individuals to contact him on that telephone number. This number was also identified by multiple MFFCU vishing victims. There were multiple sources of payment, which included MFFCU debit card numbers ending in

2180 and 4410. In the transaction histories, there were multiple transfers which were identified as being related to the funnel accounts identified by MFFCU Corporate Security. This included transfers from Veronica Murrillo using MFFCU debit card ending in 3236 and Maranda Orner using MFFCU debit card ending in 0447. There were additional transfers to and/or from the accounts of Top Don, Courtney B. and Juanita Larmer. Also identified was the $250 transfer made from the Facebook user "Fourthe Lowautosales" on February 17, 2023. This user sent Lewis $250 in exchange for being taught how to scam.

The Cash App cash tag $timmykatu was identified via telephone number 717-602-3741. This phone number was identified by Lewis as a point of contact in social media messages, as well as by MFFCU vishing victims. The account is registered to an Emmanuel Soto, who was a reported vishing victim by MFFCU. The address utilized on the account is 300 Lincoln Street, Steelton, PA. There were two payment sources added to the account that were identified as Citizens Bank and PNC Bank debit card numbers. Within the transaction history your Affiants identified multiple transfers to and/or from Cash App accounts for Jorge-Cruz Espinoza, Courtney B, Christian, E Foreign Rodriguez, Max Porter, Abanoub, and Jwett Milly. The payment source for E Foreign Rodriguez was identified as MFFCU card ending in 6623 which is owned by Esmelda Rodriguez. The payment source for Max Porter was identified as MFFCU card ending in 0284, which according to MFFCU was issued to Ijamiere McKinney. Mckinney was identified as a MFFCU funnel account. The payment source identified for Abanoub was MFFCU card ending in 5781. The payment source for the transfers made by Jwet Milly was identified as MFFCU card ending in 2114, which was issued to Owen Grogan. Grogan was identified as a MFFCU funnel account.

Through social media messages involving Lewis and witness interviews, the Cash App tag $murphy3xxx was identified. The records show the account was registered using telephone number 717-943-4208, which Lewis also identified as a point of contact in social media messages. The IP Address 172.58.208.78 was identified based on legal service for Lewis's Instagram account and was used to access this Cash App account on multiple occasions.

There were multiple sources of payments identified as being added to the account from numerous financial institutions. These payment sources included the MFFCU debit card ending in 4817, which was identified as being issued to Tyreek Rush. Rush's MFFCU account was identified as a funnel account. In addition, there were multiple transfers conducted between this account and other individuals whose accounts were flagged for fraudulent activity by MFFCU Corporate Security. These include transfers from a Cash App account identified as Alyssa with the payment source being a MFFCU debit card ending in 6665. This debit card was identified as being issued to victim Robert Strahosky. Honesti Bellamy was identified as sending funds to the account using MFFCU card ending in 8533. This card was identified as being issued to Nathan Fetrow, who reported attempted fraudulent activity on the card to MFFCU. Janae Jackson attempted to transfer funds using payment source identified as MFFCU debit card ending in 4894. This card was issued to Robert Gabryszewski and reported by him as having fraudulent transactions to MFFCU. Teresa Arment utilized MFFCU debit card ending in 0872 to transfer funds to the account. This card was confirmed as being issued to Arment by MFFCU. In addition, there were transfers between '$murphy3xxx', 'Courtney B', and '#spreadgang'. The '#spreadgang' account was identified as Cash Tag '$fhnarden', which was identified as Cash App account registered to Avery McCollum Jr.

Your Affiants reviewed the Cash App records for the account identified as $fnharden. The Display Name of this account was identified as '#spreadgang' with telephone number 717-963-1243. This account was identified on witness bank statements as having received funds transfers, in addition to the identification of transfers between this account and that of '$murphy3xxx'. Witness #3 was originally requested to transfer funds to '$murphy3xxx' but the transfer was denied. The account records show that Witness #3 had funds transferred from their MFFCU account to the MFFCU account of Avery McCollum, Jr. The funds were then transferred from McCollum Jr's MFFCU to the Cash App account identified as '#spreadgang'. In the review of records, there were numerous payment sources added to the Cash App account, which included MFFCU debit card ending in 6343. The debit card ending in 6343

was identified as being issued to McCollum, Jr. In addition there were multiple transfers between this account and the Cash App accounts identified as Robinjwetts (this account was identified as being owned by Carl Gonzalez), Heidi Murphy, and Don Deno. In addition there were transfers from Nathan Jackson with payment source identified as MFFCU card ending in 6472. Jackson was identified as a funnel account by MFFCU Corporate Security.

The Cash App account of Carl Gonzalez was identified as Cash Tag $hellarackies. This account has had multiple Display Names, which included Austin Gomez, Dustin Miller, Carl Gz, Bossedupsav, and Robinjwetts. The telephone numbers attached to this account were identified as 215-888-9956 and 717-963-4228. There were approximately 34 payment sources linked to this account from multiple financial institutions, which included PNC Bank, Citizens Bank, MFFCU, and JP Morgan Chase. There were four MFFCU debit cards attempted to be added to the account, which were identified as MFFCU debit cards ending in 6587, 6343, 7894, and 3311. A debit card ending in 6587 was identified as being issued to Witness #3, a debit card ending in 6343 was identified as being issued to Avery McCollum, Jr., a debit card ending in 7894 was identified as being issued to Ericka Carter, and a debit card ending in 3311 was identified as being issued to Gonzalez. Carter was identified by MFFCU Corporate Security as a funnel account. There were a large amount of transfers between Gonzalez and other identified individuals, which included the MFFCU funnel accounts of Terrel Simons, Trequan Porter, Jesse Yepes, Kira Witness #7, Joel Davis, Darryl Martin, Aniya Smith, Denzel Outen, Ericka Carter, Dream Moore, Myhkail Stubbs, and Owen Grogan. In addition there were transfers with the Cash App accounts identified as Lachelle (Monserrat), Courtney B, #spreadgang, and Asiaa. The payments ranged from $50 to $2,000, which fit the pattern of payments required for the funnel account owners to participate in the fraud scheme.

IX. Toll Analysis

Members 1st Federal Credit Union vishing victims reported receiving phone calls from individual(s) impersonating the MFFCU fraud department from telephone numbers 717-943-4208, 223-269-3859, 717-602-3741

717-421-8450, 717-908-7176, 717-307-7472, and 775-430-6123. Through the course of your Affiants' investigation, these telephone numbers were identified as being utilized by Tyreese Lewis through a review of social media messages and service of legal process during the time frame of the investigation. Your Affiants reviewed the toll records of the aforementioned telephone numbers, which confirmed the MFFCU vishing victims received the reported phone calls on or about the dates, the fraudulent activity was reported to MFFCU Corporate Security.

A review of the records provided by MFFCU Corporate Security show additional vishing victims, who were contacted via spoofed phone numbers to make it appear as though the impersonator was calling from MFFCU. The subscriber records obtained for the identified telephone numbers indicate they are prepaid cell phones. Your Affiants know based on training and experience that individuals are not required to provide identifying information at the time of purchase, which could result in the use of fictitious names and/or business names being registered to the telephone numbers. There were two telephone numbers, identified as 717-421-8450 and 717-421-1054, which show the registered subscriber as Members First Federal Credit Union. Registering phones in this manner could result in Members First Federal Credit Union being displayed on the victim's caller ID.

X. Conclusion

Between August 1, 2022 through present, your Affiants identified Tyreese Lewis, Carl Gonzalez, Zyaire Monserrat, Jaire Cotton, Tanayia Gottshall, Lavon Whitaker, Kristopher Davis, Eric Greenawalt, Ricky Cruz, Robert Rodriguez, Cyrai Tillman, Corey Gray, Derek Jones, and others yet to be identified as conspiring to commit the crimes of Corrupt Organizations, Dealing in Proceeds of Unlawful Activities, Identity Theft, Access Device Fraud, Forgery, Theft by Deception, Theft by Unlawful Taking, Computer Trespass and other related offenses. These offenses occurred throughout the South Central Pennsylvania region to include Dauphin, Cumberland, York, and Lancaster counties. The majority of the criminal activity occurred in Dauphin County to include fraudulent point

of sale transactions, cashing of forged checks, and withdrawals of stolen funds from funnel accounts. Additionally, many of the Identity Theft victims and funnel account owners live in Dauphin County.

As of July 14, 2023, your Affiants identified the total exposure of fraudulent activity to be approximately $1.8 million dollars. Your Affiants have identified approximately $1.3 million dollars in losses to Members 1st Federal Credit Union and other victims of Identity Theft and Access Device Fraud. The loss amount and number of identified victims is expected to increase as records from additional financial institutions are secured.

Your Affiants respectfully request a warrant for arrest be issued to Tyreese Lewis. Your Affiants respectfully request to have this warrant sealed to protect the integrity of this investigation as the activity is ongoing and co-conspirators continued to be identified through victim and witness interviews and collect evidence, which may be otherwise destroyed.

I, KATHRYN GRADY AND CHRISTOPHER COLARUSSO (PSP), BEING DULY SWORN ACCORDING TO THE LAW, DEPOSE AND SAY THAT THE FACTS SET FORTH IN THE FOREGOING AFFIDAVIT ARE TRUE AND CORRECT TO THE BEST OF MY KNOWLEDGE, INFORMATION AND BELIEF.

I CERTIFY THAT THIS FILING COMPLIES WITH THE PROVISIONS OF THE *CASE RECORDS PUBLIC ACCESS POLICY OF THE UNIFIED JUDICIAL SYSTEM OF PENNSYLVANIA* THAT REQUIRE FILING CONFIDENTIAL INFORMATION AND DOCUMENTS DIFFERENTLY THAT NON-CONFIDENTIAL INFORMATION AND DOCUMENTS.

KG TM for/Colarusso
(Signature of Affiant)

Sworn to me and subscribed before me this 26th day of July 2023

Date Jean E. Cullo, Magisterial District Judge

My commission expires first Monday of January,
2030

COURT OF COMMON PLEAS SEAL DAUPHIN COUNTY, PA