

DEPARTMENT OF JUSTICE

ElderJustice INITIATIVE

Tackling Transnational Robocall Scams

The Importance of Local, State and Federal Partnerships

APRIL 13, 2021



Housekeeping

- Today's webinar will be recorded. You will be provided with the information from the webinar on the EJI website.
- All attendees will enter the webinar in listen-only mode.
- If you have questions, type them in the chat box. We will do our best to address them during the webinar, but if we cannot, they will be addressed during the Q&A session before we conclude the webinar.
- Closed captioning is provided in the pod below the presentation. If you are having issues viewing closed captioning and do not have the Adobe Connect app installed on your computer, please close out this meeting, download the Adobe Connect application, and then rejoin the webinar. If you do not wish to download the app, close out of the webinar, make sure Adobe Flash is enabled on your web browser, rejoin the meeting, and then click on the link "join with classic view."



ELDER JUSTICE INITIATIVE

The mission is to support and coordinate the U.S. Department of Justice's enforcement and programmatic efforts to combat elder abuse, neglect, and financial fraud and scams that target older adults.

The EJI does so by

- promoting justice for older adults;
- helping older victims and their families;
- enhancing state and local efforts through training and resources;
- supporting research to improve elder abuse policy and practice.

ELDERJUSTICE.GOV

You're fighting elder abuse on the front lines. We've got your back.

The mission of the Elder Justice Initiative is to support and coordinate the department's enforcement and programmatic efforts to combat elder abuse, neglect, and financial fraud and scams that target our nation's seniors.



COPS.USDOJ.GOV

You're fighting on the front lines. We've got your back.

The Office of Community Oriented Policing Services (COPS Office) is the component of the U.S. Department of Justice responsible for advancing the practice of community policing through information and grant resources.



Community Oriented Policing Services
U.S. Department of Justice



POLL QUESTION

What is Your Professional Affiliation?

Adult protective services

Aging services

Civil legal services

Financial services/industry

Health care services

Law enforcement

Long-term care ombudsman

Mental health services

Other government agencies

Prosecutor

Research

Victim services

Other

POLL QUESTION

What is your level of experience working in elder justice?

- None to a little experience
- Somewhat experienced
- Extremely experienced

Speakers

Jolee Porter

Assistant U.S. Attorney, Northern District of Georgia, detailed to the Transnational Elder Fraud Strike Force at the US DOJ Consumer Protection Branch

Jon Heslep

Senior Special Agent, Office of Inspector General, Social Security Administration

Margaret Moore

Detective, Aiken Department of Public Safety, Aiken, South Carolina



Sample Victim Story

- CM, **70 years old**, of Illinois.
- Callers **impersonating federal agents** said her **SSN was involved in crimes** and she would be arrested.
- Scammers called numerous times a day from Sept. to Nov. 2019.
- CM **mailed \$286,000** via FedEx to SC, CA, NJ, and FL.
- She reported the scam to LE in Nov. 2019 and was **hospitalized** soon thereafter.



Older Americans Are Prime Targets

2020

Younger people reported losing money to fraud **more often than older people.**

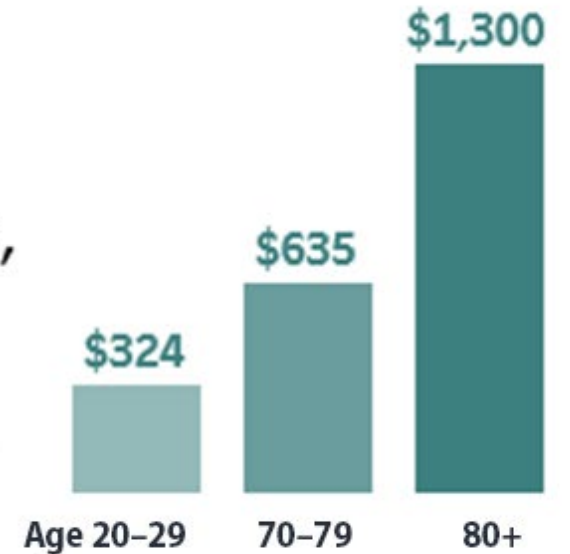


Age 20-29



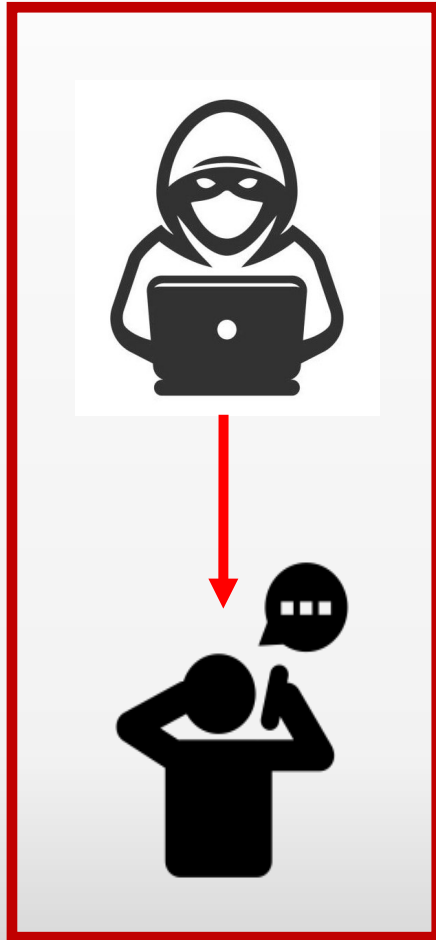
Age 70-79

But when people aged 70+ had a loss, **the median loss was much higher.**





The Scams



- Company imposter
- Grant / Payday loan
- Government imposter
(*SSA, IRS, USMS, USCIS*)
- Lottery / Sweepstakes
- Tech support
- And others . . .



How Call Centers Contact Victims

- Purchase VoIP phone numbers from U.S.-based telecommunication providers and TextNow
- Overseas call centers “spoof” legitimate phone numbers to appear legitimate
- Thousands of voicemails left for victims to “self-select”
- Victim calls routed overseas to foreign call centers





Primary Vehicles for Scammed Funds



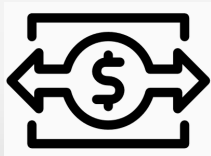
- Bank transfers



- Gift cards



- Mailed cash



- Wire transfers (MoneyGram, Western Union, RIA)



United States v. Patel et al.



ORIGINAL Case 1:20-cr-00204-UNA Document 19 Filed 06/09/20 Page 1 of 5

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

FILED IN OPEN COURT
U.S.D.C. - Atlanta
JUN - 9 2020
By: JAMES N. HAYDEN, Clerk
Deputy Clerk

UNITED STATES OF AMERICA

v.

MEHULKUMAR MANUBHAI PATEL AND
CHITALI DAVE

CRIMINAL INDICTMENT No.

1:20-CR-204

THE GRAND JURY CHARGES THAT:

COUNT ONE

(Conspiracy to Commit Money Laundering - 18 U.S.C. § 1956)

At all times relevant to this Indictment:

1. As used in this Indictment, a "call center" was an organization or group of organizations based in India that defrauded U.S. residents, including the elderly, by misleading victims over the telephone into sending money utilizing scams such as tech support and Social Security number scams.
2. As part of the tech support scam, India-based call centers would induce the victims to send money in exchange for supposed technical support for their computers. The callers would then provide nothing in return. At times, callers misled the victims into providing remote access to their computers. The callers then would access the victims' bank accounts. The callers routinely misled the victims by making it appear as though the caller accidentally added money to the victims' bank accounts. The callers would then instruct the victims to send cash through common carriers, such as FedEx and the United Parcel Service (UPS), to aliases used by other members of the fraud network.
3. As part of the Social Security number scam, India-based call centers posed as federal agents in order to mislead victims into believing their Social

- SSA and tech support imposter scams
- More than \$600K lost; dozens of victims
- Federal investigation by SSA—OIG with NDGA USAO
- State and local LE were key to case's success



Victim Report



- 54-year-old from Ohio with seizure-induced brain damage
- Defrauded by Indian caller pretending to be **tech support**
- Provided **remote access** to computer, bank account
- Caller made it appear as though money was added to his account
- Victim “returned” **\$10,000 via UPS** to “Davis Jeck”
- **Reported fraud** to Westlake (Ohio) Police



Follow the Money





Follow the Money




**AIKEN
PUBLIC
SAFETY**

**ADPS had UPS divert
packages to UPS Store**



Build the Case: Tracking & Surveillance



The image shows a screenshot of the UPS tracking website. At the top, there is a navigation bar with the UPS logo and the text "United States". Below this, there are links for "My UPS" and "Shipping". A search bar contains the text "Tracking Number" and a "Track" button. The tracking number "9274890105300536469775" is displayed in a green box and is circled in red. Below the tracking number, it says "Delivered by Local Post Office". Further down, it indicates "Delivered On: Saturday, 04/12/2014 at 6:15 P.M." and "Left At: USPS". At the bottom, there is a section for "Additional Information" with fields for "Package Actual Weight", "Package Delivery Date", "Package Destination", "Package ID", "Package Sequence Number", and "Package Status".





Build the Case: Interviews



- To whom do they report?
- Where is the money transferred to/from?
- What other aliases and addresses do they use?
- What is the conspiracy duration?
- Are there other conspirators?
- Does LE have consent to search?



Follow the Money



\$20,000 immediately
intercepted and
returned to victims



Build the Case: Find Other Victims

- \$10,000 → more than \$600,000
- Subpoena common carriers for all packages sent to
 - Addresses used by your target(s)
 - Aliases used by your target(s)





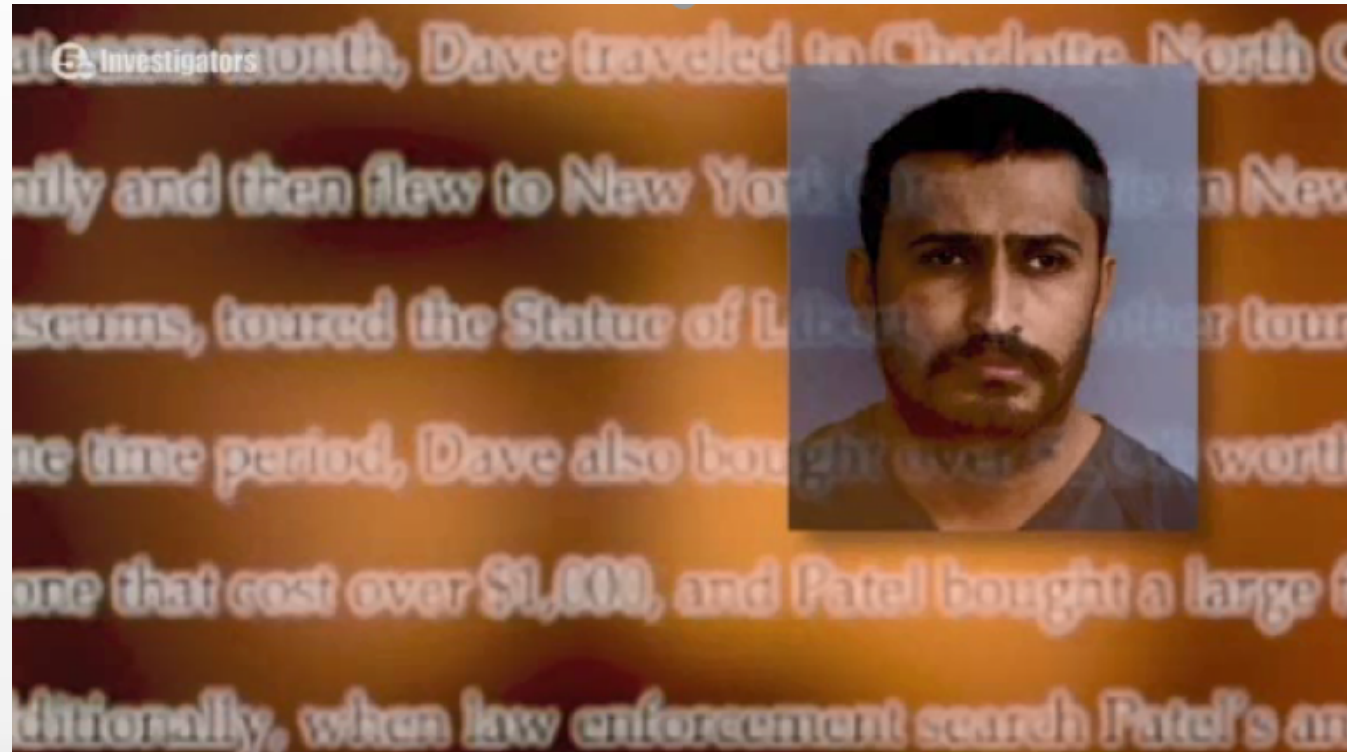
Build the Case: Phones



- Pictures of fake IDs
- Tracking info
- Messages with scam leaders and co-conspirators (WhatsApp)
- Videos/Pictures of money
- Evidence of spending



Build the Case: Phones





Build the Case: Premises Searches



- Fake IDs
- Cash
- Phones
- Lead lists



Evidence of Knowing Participation

- Use of **fake IDs**
- Receiving large sums of **cash**
- Going from **place to place** to avoid detection
- **Serially open/use bank accounts** to send/receive money
- Has been **warned** by bank or law enforcement



Criminal Charges

- **State**
 - **Obtain property under false pretenses (S.C. § 16-13-240)**
- **Federal**
 - **Concealment Money Laundering (18 U.S.C. § 1956)**
 - **Mail Fraud or Wire Fraud (18 U.S.C. §§ 1341, 1343)**
 - **Unlicensed Money Transfer Business (18 U.S.C. § 1960)**



What If They Are Unwitting?



Law Enforcement
Atlanta Division
123 Money Mule Way
Atlanta, GA 30341

HAND-DELIVERED

Ms. Money Mule,

Law enforcement is providing warning that you, and/or persons you associate with, may be engaged in fraudulent activity that violates state and/or federal criminal laws. Specifically, your recent transmission or receipt of money via wire transfer, bank transfer, postal service, cashier's check, electronic deposit, and/or gift cards may have facilitated the transfer of money from the victims of a crime to the perpetrators of a fraudulent scheme.

Some fraudulent schemes involve criminals who falsely represent themselves as someone else, in order to trick victims into sending money via wire transfer to an identified pre-determined account (e.g. your Bank Account Ending in 1234). The criminal may ask the account holders, such as yourself, to "process payments", "transfer funds", or "re-ship products" to facilitate the movement of money obtained through fraud from victims to the criminals. These requests may be masqueraded as work from home employment, secret shopper opportunities, online romances and relationships, lottery winnings, or import taxes.

Under certain circumstances, knowingly engaging in a financial transaction that involves funds derived from illegal activity may violate the federal money laundering laws, even if you had no involvement in the underlying criminal activity. Under certain circumstances, you may also have a legal obligation to inquire about the source of the funds and may not avoid legal responsibility by being willfully blind to the source of funds. A knowing and intentional violation of the money laundering laws may result in criminal prosecution and the seizure of property that is found to be tainted by illegal funds. By agreeing to engage in such transactions, you may be also be facilitating a fraudulent scheme and assisting the perpetrators of the scheme.

The FBI has documented the delivery of this letter to you. Along with this letter, the FBI has also explained to you the precise financial transaction(s) in which you engaged that may have involved illegal funds. Receipt of this letter will be taken into consideration, should you continue to be involved in the type of activities described above.

I signed this letter voluntarily _____ (Initials) Date: _____

Recipient Name: _____ (Printed)

_____ (Signature)

WARNING LETTER: Knowingly transferring funds derived from illegal activity **may be a crime**, even if you had no involvement in the underlying criminal activity.

Money mules help international criminal networks steal money from senior citizens, businesses, and people just like you.

#DontBeAMule





Where to Report?



FEDERAL BUREAU OF INVESTIGATION
Internet Crime Complaint Center IC3



Cyber cases: ic3.gov



FEDERAL TRADE COMMISSION
ReportFraud.ftc.gov



Free Education Materials



FEDERAL TRADE COMMISSION
Free Publications for America's Consumers

www.ftc.gov/bulkorder

? Want to know more? Sign up for scam alerts at ftc.gov/subscribe.

...PassItON

Imposter Scams



Here's how they work:

You get a call or an email. It might say you've won a prize. It might seem to come from a government official. Maybe it seems to be from someone you know – your grandchild, a relative or a friend. Or maybe it's from someone you feel like you know, but you haven't met in person – say, a person you met online who you've been writing to.

Whatever the story, the request is the same: wire money to pay taxes or fees, or to help someone you care about.

But is the person who you think it is? Is there an emergency or a prize? Judging by the complaints to the Federal Trade Commission (FTC), the answer is no. The person calling you is pretending to be someone else.

Here's what you can do:

1. **Stop. Check it out – before you wire money to anyone.** Call the person, the government agency, or someone else you trust. Get the real story. Then decide what to do. No government agency will ever ask you to wire money.
2. **Pass this information on to a friend.** You may not have gotten one of these calls or emails, but the chances are you know someone who has.



Please Report Scams

If you spot a scam, please report it to the Federal Trade Commission.

- Call the FTC at 1-877-FTC-HELP (1-877-382-4357) or TTY 1-866-653-4261
- Go online: ftc.gov/complaint

Your complaint can help protect other people. By filing a complaint, you can help the FTC's investigators identify the imposters and stop them before they can get someone's hard-earned money. It really makes a difference.



Federal Trade Commission | ftc.gov/PassItOn



Contact Information

AUSA Jolee Porter
Jolee.Porter2@usdoj.gov

Senior S/ A Jonathan E. Heslep
Jonathan.Heslep@ssa.gov

Detective Margaret Moore
MMoore@CityofAikenSC.gov

DEPARTMENT OF JUSTICE

ElderJustice INITIATIVE

Questions

elder.justice@usdoj.gov



Poll Question

How helpful did you find this webinar?

- Very helpful
- Somewhat helpful
- Not at all helpful