Michigan State Police Computer Crimes Unit
Internet Crimes Against Children Taskforce

Detective Sergeant Thomas Gladney III

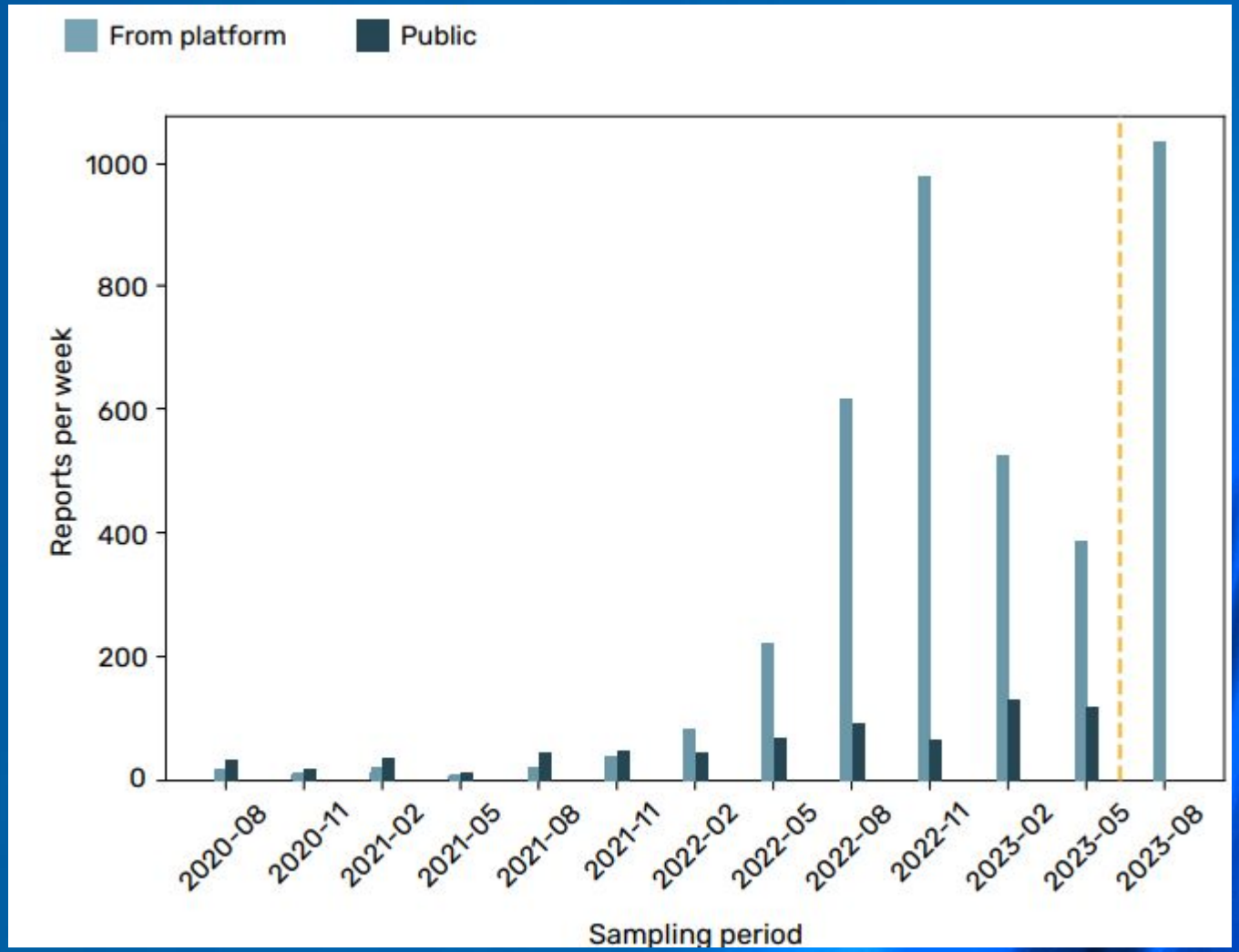
ICAC
Internet Crimes Against Children
Training & Technical Assistance Program

ICAC
Internet Crimes Against Children
Training & Technical Assistance Program

What is Sextortion?

Extortion in which a perpetrator threatens to expose sexually compromising information (such as sexually explicit private images or videos of the victim) unless the victim meets certain demands

Sextortion Cases Per Week



ICAC
Internet Crimes Against Children
Training & Technical Assistance Program

The Process

Fastest Growing Cyber Threat

- According to the United States Department of Justice, ‘Sextortion’ is labeled as the most important and fastest-growing cyber threat to children, with more minor victims per offender than all other child sexual exploitation offenses.

- Justice Department warns of dramatic increase in ‘Sextortion’ schemes targeting boys.

Perpetrator Motivations

- Financial Gain
  - It's their JOB
- Fulfilling Sexual Desires
  - Sexual gratification
- Revenge
  - Bad relationship breakup
- Humiliation

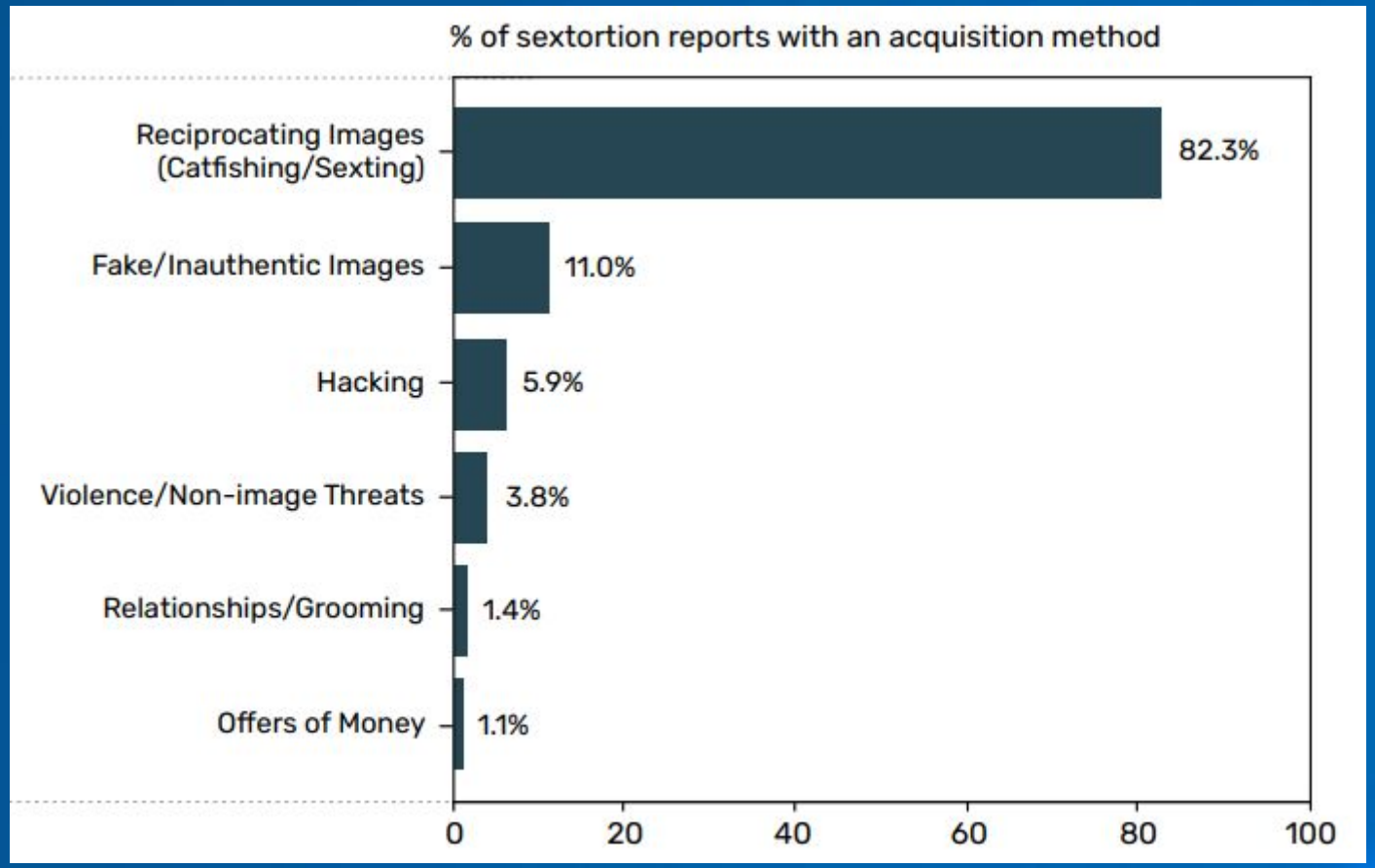
In an earlier analysis, the dominant motive of offenders was to get more explicit images of a child, but in reports from early 2022, **79%** of the offenders were seeking money.

Trends – What it looks like

- Most victims are between age 14 and 17, but kids as young as 6 have been targeted
- Fake accounts vs. Hacked accounts
- Screen recording vs. sending
- 14-17 Year Old Males (90%)
- $500 average amount

Not weeks. Not days. HOURS

How Sextortion Images are Obtained



Applying Pressure

- Exaggerating the impact of these images going out is the primary method of applying pressure
  - Parents/Grandparents
  - Post on school social media
  - Employers
  - “Viral”

Case Example - Jordan DeMay

- Hacked Instagram account
- Catfish, “she” sent nude images first
- Demanded $1000 to not send the content
- Paid $300, but more was demanded
- “You win, I’m going to Kill Myself” approximately 6 Hours since contact

Change in Approach by Law Enforcement

- Child Sexually Abusive Material Possession / Distribution is a common problem in schools
- Previous methods involved deterrence by educating students on criminal penalties
- Current methods stress that if a child finds themselves in a sextortion situation, law enforcement is focused on the suspect

Perpetrators

- Majority of suspects are from other countries
  - Primarily West Africa/Southeast Asia
- "Shotgun Method" vs. Targeted approach
- Making payments does not typically end contact

Sextortion Red Flags

- Friend/Message requests from unknown persons
- Pressure to engage in explicit image sharing or video chatting (usually shortly after the conversation begins)
- Moving the conversation from one platform to another
- Broken English / Poor Grammar

Prevention

- Avoid engaging in explicit online interactions
- Ensure social media privacy settings are on their highest settings
- Talk with children before anything happens, let them know it is safe to report something like this.
- Education prior to being contacted is vital for this type of crime. There may be limited time to address the issue after it happens.

Social Media – Privacy and Safety

- Snapchat
  - Family Center
- TikTok
  - Family Pairing
- Meta (Facebook / Instagram)
  - Education Hub

Steps For The Victim

- Stop engaging with the blackmailer
- Block the suspect, but do not delete any messages
- Report the account on the platform
- Report the sextortion to police AND NCMEC's Cyber Tipline (www.cybertipline.org)
- Go to Take it Down at "takeitdown.ncmec.org" for help removing images from the internet.

Take It Down

Get Started | Resources and Support | About Us | Participants | FAQ | English (English)

Take It Down.

Having nudes online is scary, but there is hope to get it taken down.

This service is one step you can take to help remove online nude, partially nude, or sexually explicit photos and videos taken before you were 18.

Get Started +

ICAC
Internet Crimes Against Children
Training & Technical Assistance Program

Best Approach

- **EDUCATE**
  - Be proactive
  - Community Engagement (Schools, parents, public officials)
  - What are the trends in your area?
    - We have had to change some of our strategy
  - It will always be evolving
- Too many tips/reports for law enforcement

Sextortion VS Child Exploitation

- Targeting methods are very similar
- Likely victims have similar characteristics
- Contact will look different and have different red flags
  - Use information/content to build trust relationship as opposed to extortion
  - Longer period before sexualizing relationship (possibly)
  - More likely to involve flattery/gifts

www.MichiganICAC.com

MICHIGAN

Internet Crimes Against Children Task Force

1-877-MI-CYBER

1-877-642-9237

Home About Us Resources Press Releases

Internet Safety Resources

YOUTH

NetSmartz

KidSmartz

NSTeens

OK2SAY

No Filtr

Love146

PARENTS

Connect Safely

Cyberwise

Sexting Tips for Parents & Youth

Protect Young Eyes

Protect MI Child

Chrome Book Safety

Safety Pledge

Common Sense Media

ICAC Internet Safety Video

GENERAL

Mobile Apps Guide

Dept. of Homeland Security- Blue Campaign

Safer Internet Day

Take It Down

Civilian/Citizen options

- Contact LE / Parents if underage
- NCMEC report at missingkids.org or 1-800-THE-LOST (1-800-843-5678)
- Have victim cease communication, obtain identifying info for LE
- DO NOT support sending of money/items
- Help victim obtain emotional and mental support

Steps for Law Enforcement

- Obtain identifying info
  - Requested financial app and info related to
  - Username
  - Phone number
  - Email
  - Etc…
- Preservation to account
  - Victim(s) and suspect
  - Search.org

SEARCH

ICAC
Internet Crimes Against Children
Training & Technical Assistance Program

Steps for Law Enforcement (cont.)

- SW to account for:
  - IP / Other identifying information
  - Location data
  - Other potential victims
  - Note any language dialect for location-if possible
  - Banking/credit cards
- Get social media/phone download from victim
- Emotional/mental support for victim

Related Statutes – Victim Under 18

- MCL 750.145c(2) – Child Sexually Abusive Activity
- MCL 750.145c(3) – Distribute CSAM
- MCL 750.145c(4) – Possess CSAM
- MCL 752.797(3) – Use of a Computer to Commit a Crime

Related Statutes – Victim Over 18

- MCL 750.145e – Dissemination of sexually explicit material
  - Requires distribution, intent to threaten, coerce, intimidate
  - Misdemeanor
- MCL 750.213 – Extortion
  - Requires threat of injury or accusation of a crime

Sources

- Thorn and National Center for Missing and Exploited Children (NCMEC). (2024). Trends in Financial Sextortion: An investigation of sextortion reports in NCMEC CyberTipline data
- *Cybertipline Data* (no date) *National Center for Missing & Exploited Children*. Available at: https://www.missingkids.org/cybertiplinedata

D/Sgt. Thomas Gladney
269-845-0994 – GladneyT@Michigan.gov

The **Michigan State Police – Internet Crimes Against Children Task Force** encourages parents and/or guardians to take an active role in their children's internet safety.

For more information, safety tips, or to report inappropriate cyber behavior, visit:

- MichiganICAC.com
- Missingkids.org
- Cybertipline.org
- ProtectYoungEyes.com
- OK2Say.com
- TakeItDown.ncmec.org

Call 1-800-THE-LOST