Investigator's Office, Laboratory, & Forensic Certification

Nelson Chapter 2 plus additional material

(continued from lecture 3)

Assignments Posted

Assign02b_s

- *Complete the Forensic Imaging Lab*
- *Follow the instructions attached to the assignment*
- *Due: Sunday 18 September @ 11:59pm (US Central)*

Assign03a_s

- *Repair files based on their (file signatures)*
  - Will use skills we demonstrated in Clownfish lab
  - Cleaned file will be next assignment (Assign03b_rds)
- *Two attachments*
  - Instructions for the Assign03a_s
  - The file you are to repair/clean (Assign03b_rds)
- *Due: Monday, 26 September @ 11:59pm (US Central)*

Assign03b_rds

- *Follow instructions in repaired file*
- *Due: Sunday, 2 October @ 11:59pm (US Central)*

Uniform Crime Reports (UCR)

UCR Overview

U.S. crime statistics are reported and categorized in a standard way

Started in 1930

Recommended by International Association of Chiefs of Police

FBI receives the data from many local law enforcement agencies

FBI generates a semiannual UCR based upon this info

Today the UCR is based upon data provided by about 18,000 law enforcement agencies

All crime; not just high tech

UCR Overview

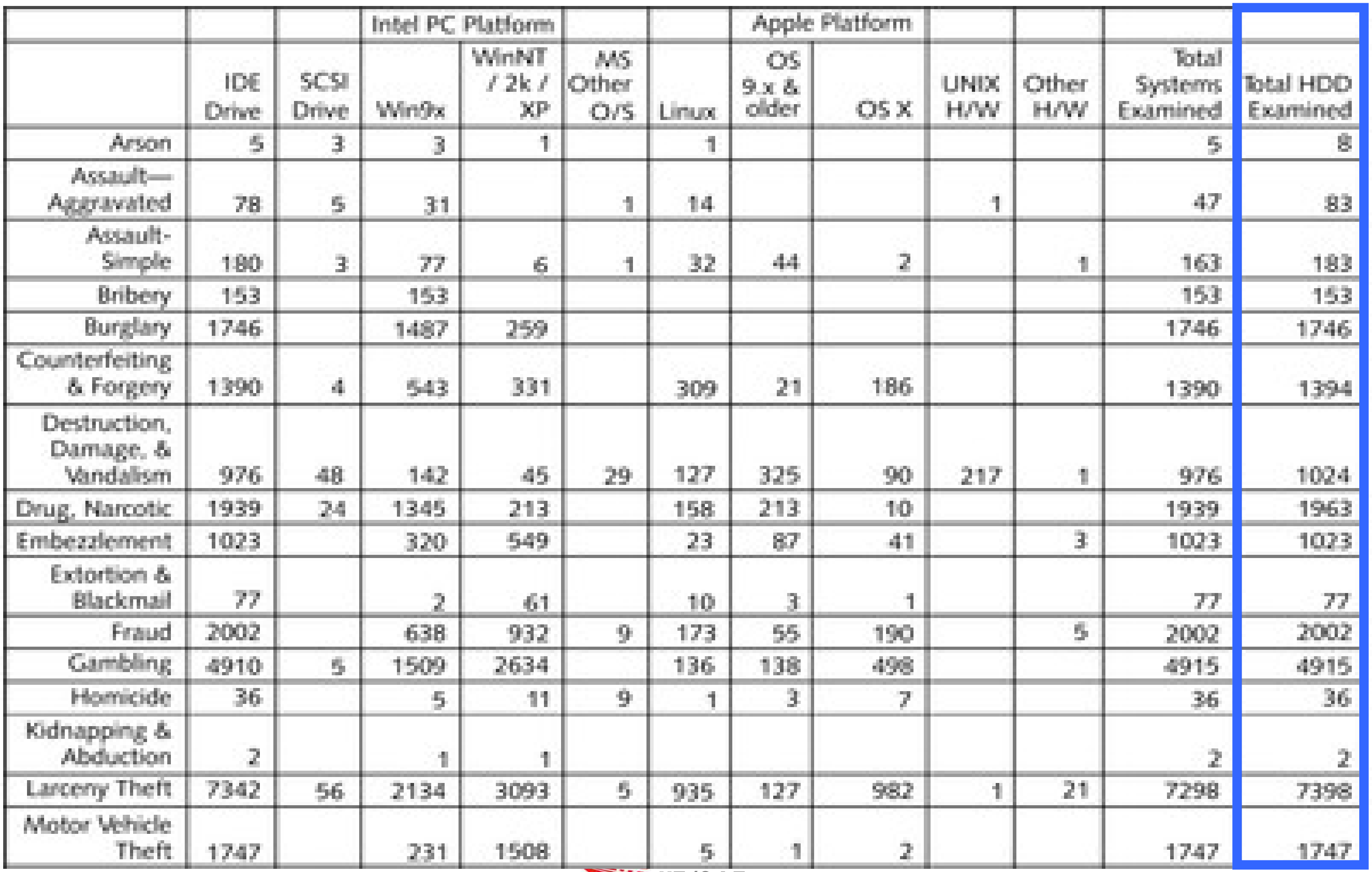
- Data is reported in a specific way
  - *By location, specific crime classifications*
  - *Specific ways to characterize each crime category in terms of the nature of the crime*
- FBI provides a handbook telling agencies how and what to report
- I have found it difficult to search for specific data in UCR reports
- The FBI now offers a tool called ***Crime Data Explorer***
  - *Similar interface as census data*

UCR Overview

One aspect of the UCR is information on computer crimes

The following is a sample from UCR data used in creating the UCR reports

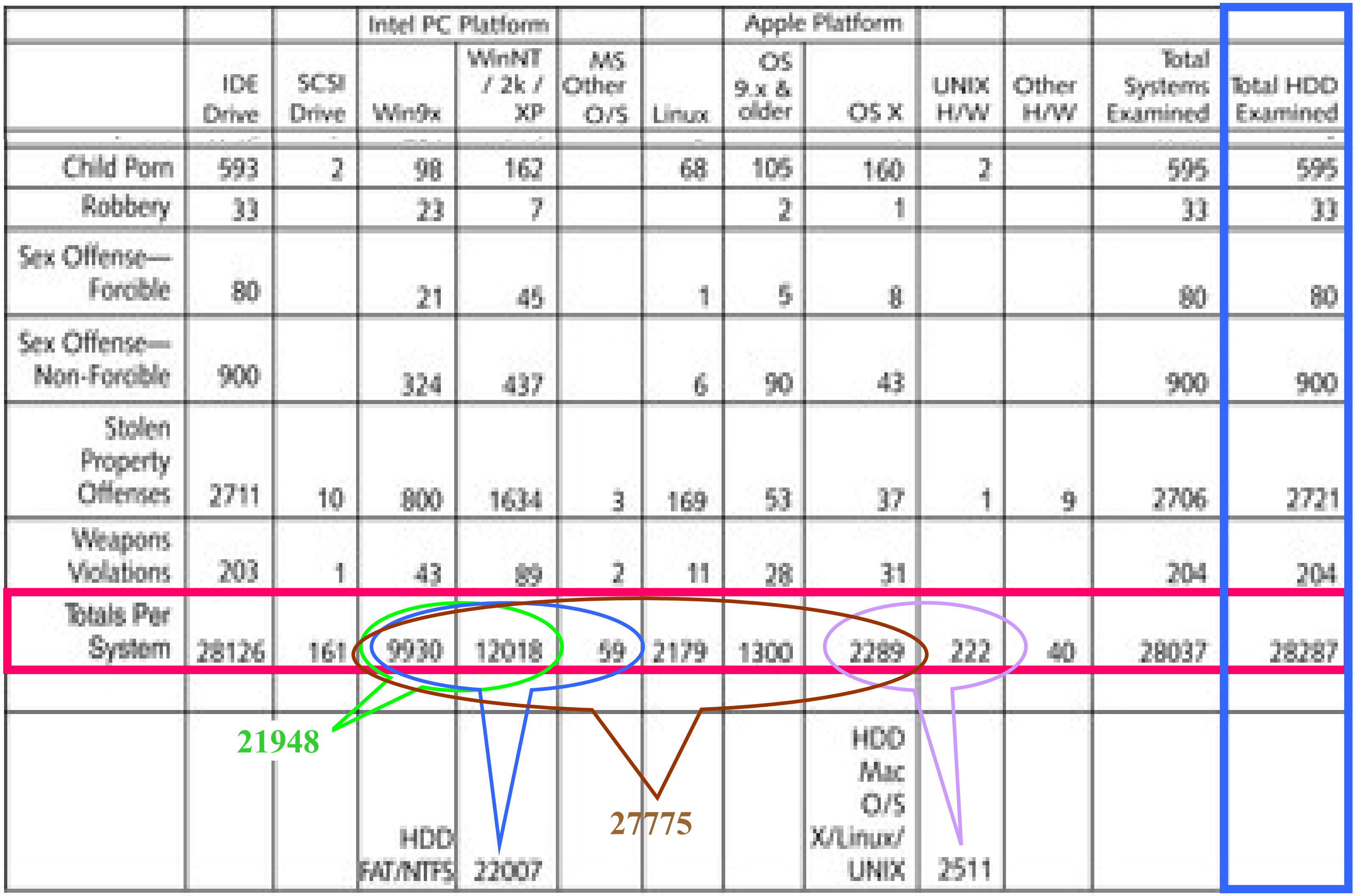
Excerpt from Older UCR Data



			Intel PC Platform				Apple Platform					
	IDE Drive	SCSI Drive	Win9x	WinNT / 2k / XP	MS Other O/S	Linux	OS 9.x & older	OS X	UNIX H/W	Other H/W	Total Systems Examined	Total HDD Examined
Arson	5	3	3	1		1					5	8
Assault—Aggravated	78	5	31		1	14			1		47	83
Assault-Simple	180	3	77	6	1	32	44	2		1	163	183
Bribery	153		153								153	153
Burglary	1746		1487	259							1746	1746
Counterfeiting & Forgery	1390	4	543	331		309	21	186			1390	1394
Destruction, Damage, & Vandalism	976	48	142	45	29	127	325	90	217	1	976	1024
Drug, Narcotic	1939	24	1345	213		158	213	10			1939	1963
Embezzlement	1023		320	549		23	87	41		3	1023	1023
Extortion & Blackmail	77		2	61		10	3	1			77	77
Fraud	2002		638	932	9	173	55	190		5	2002	2002
Gambling	4910	5	1509	2634		136	138	498			4915	4915
Homicide	36		5	11	9	1	3	7			36	36
Kidnapping & Abduction	2		1	1							2	2
Larceny Theft	7342	56	2134	3093	5	935	127	982	1	21	7298	7398
Motor Vehicle Theft	1747		231	1508		5	1	2			1747	1747

Excerpt from Older UCR Data*

(continued)



			Intel PC Platform				Apple Platform					
	IDE Drive	SCSI Drive	Win9x	WinNT / 2k / XP	MS Other O/S	Linux	OS 9.x & older	OS X	UNIX H/W	Other H/W	Total Systems Examined	Total HDD Examined
Child Porn	593	2	98	162		68	105	160	2		595	595
Robbery	33		23	7			2	1			33	33
Sex Offense—Forcible	80		21	45		1	5	8			80	80
Sex Offense—Non-Forcible	900		324	437		6	90	43			900	900
Stolen Property Offenses	2711	10	800	1634	3	169	53	37	1	9	2706	2721
Weapons Violations	203	1	43	89	2	11	28	31			204	204
Totals Per System	28126	161	9930	12018	59	2179	1300	2289	222	40	28037	28287
			HDD FAT/NTFS	22007				HDD Mac O/S X/Linux/ UNIX	2511			

21948

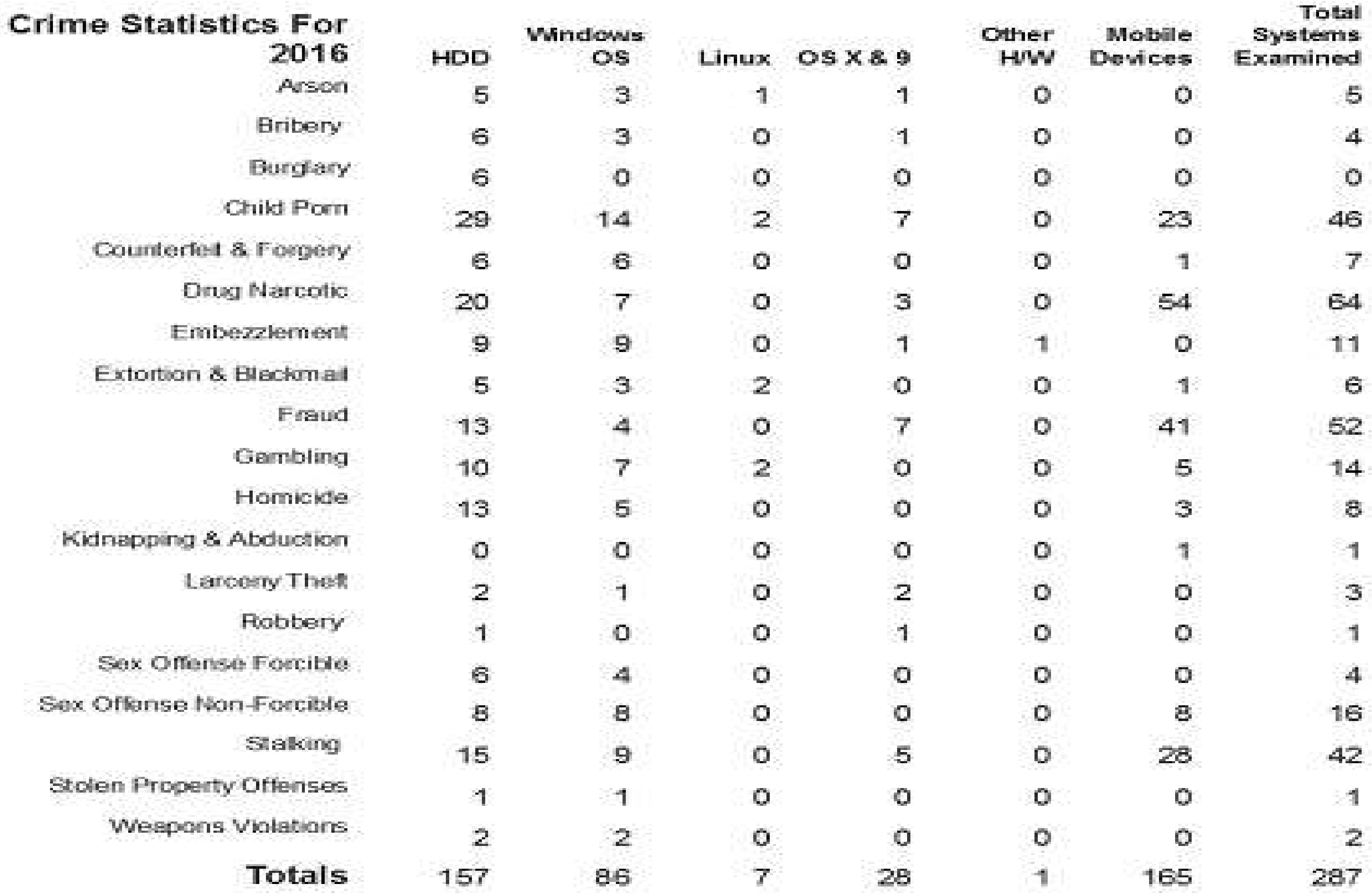
27775

Thoughts About Older UCR Data

- Windows vs. all other attacks
  - *# of crimes using Windows = 21948*
  - *# of crimes on all OSs = 27775*
  - *21948/ 27775 = ~79% of attacks were on Windows systems*
  - *What was the % of OSs that run Windows in the U.S?*
- What types of crimes are most prevalent?
  - *Larceny & theft: 26%*
  - *Gambling: 17%*
- What about sex & child porn crimes that get attention?
  - *Sex & Child Porn: 5.7%*

Table from 2016 UCR

p 67 of Nelson



Crime Statistics For 2016	HDD	Windows OS	Linux	OS X & 9	Other H/W	Mobile Devices	Total Systems Examined
Arson	5	3	1	1	0	0	5
Bribery	6	3	0	1	0	0	4
Burglary	6	0	0	0	0	0	0
Child Porn	29	14	2	7	0	23	46
Counterfeit & Forgery	6	6	0	0	0	1	7
Drug Narcotic	20	7	0	3	0	54	64
Embezzlement	9	9	0	1	1	0	11
Extortion & Blackmail	5	3	2	0	0	1	6
Fraud	13	4	0	7	0	41	52
Gambling	10	7	2	0	0	5	14
Homicide	13	5	0	0	0	3	8
Kidnapping & Abduction	0	0	0	0	0	1	1
Larceny Theft	2	1	0	2	0	0	3
Robbery	1	0	0	1	0	0	1
Sex Offense Forcible	6	4	0	0	0	0	4
Sex Offense Non-Forcible	8	8	0	0	0	8	16
Stalking	15	9	0	5	0	28	42
Stolen Property Offenses	1	1	0	0	0	0	1
Weapons Violations	2	2	0	0	0	0	2
Totals	157	86	7	28	1	165	287

Thoughts About 2016 UCR Data

Windows vs. all other attacks

- *# of crimes using Windows = 86*
- *# of crimes on all OSs = 122*
- *86/ 122 = ~70% of attacks were on Windows systems*
- *What is the % of OSs that run Windows in the U.S?*

What types of crimes are most prevalent?

Child Porn:	*18%*
Drug Narcotic:	*13%*
Fraud+Gambling:	*23%*

What about larceny & theft crimes?

Larceny Theft:	*1.3%*

So What's Changed

% Child Porn ↑ # Child Porn ↓

% Larceny Theft ↓

But what's the big elephant in the room?

Cell phones!

Internet Crime Complaint Center (IC^3)

FBI's IC^3 Overview

Originally a joint activity by FBI and NW3C

Now is an FBI operation

Mission Statement

> *To serve as a vehicle to receive, develop and refer criminal complaints regarding the rapidly expanding arena of cybercrime.*

Issues Cybercrime reports

https://www.ic3.gov

IC^3 2021 Report

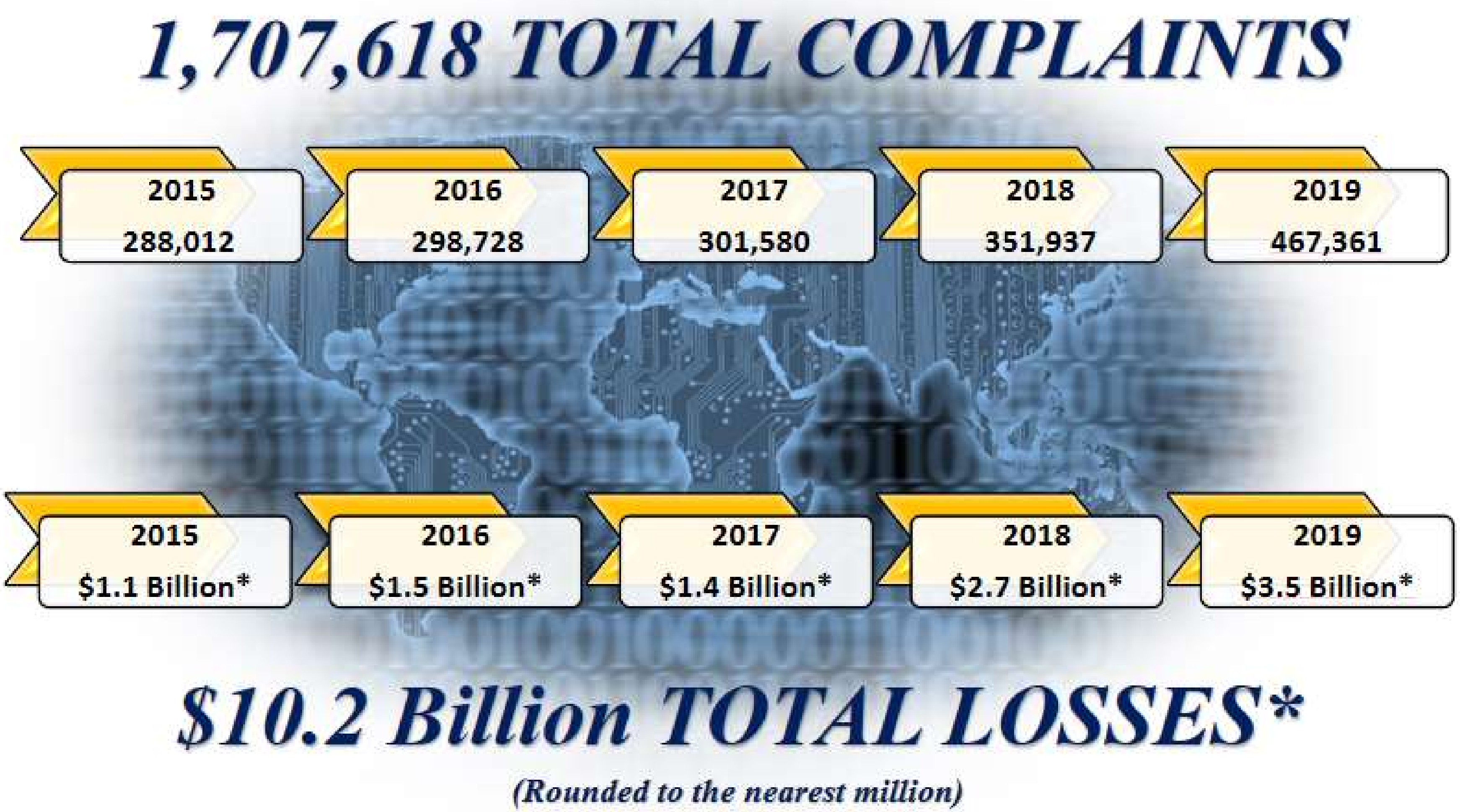
Overall Statistics

Total complaints received: 847, 376

Average complaints per day: > 2,300

Total Loss: $6.9 Billion

IC^3 2015 - 2019 Reports
Complaints Stastistics



1,707,618 TOTAL COMPLAINTS

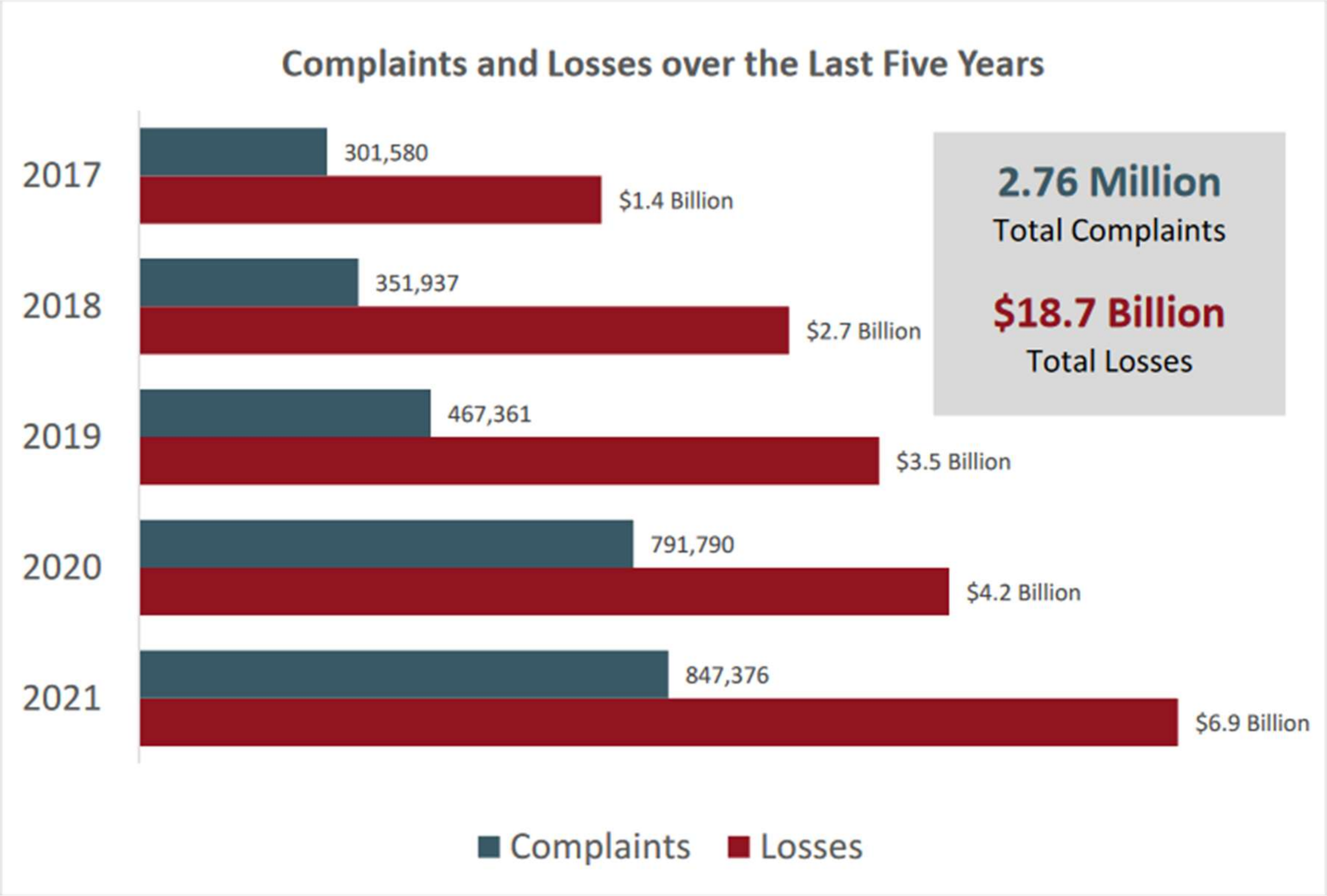
2015	2016	2017	2018	2019
288,012	298,728	301,580	351,937	467,361

2015	2016	2017	2018	2019
$1.1 Billion*	$1.5 Billion*	$1.4 Billion*	$2.7 Billion*	$3.5 Billion*

$10.2 Billion TOTAL LOSSES*

(Rounded to the nearest million)

IC^3 2017 - 2021 Reports
Complaints Stastistics



IC^3 2021 Reports
Types of Complaints

Auto

Selling vehicles that criminal doesn't own over Internet

Government Agency Impersonation

Usually via email to start

Intimidation/Extortion

Email or pop-ups allegedly from well know software firm claiming that software is infected with viruses and must be fixed immediately

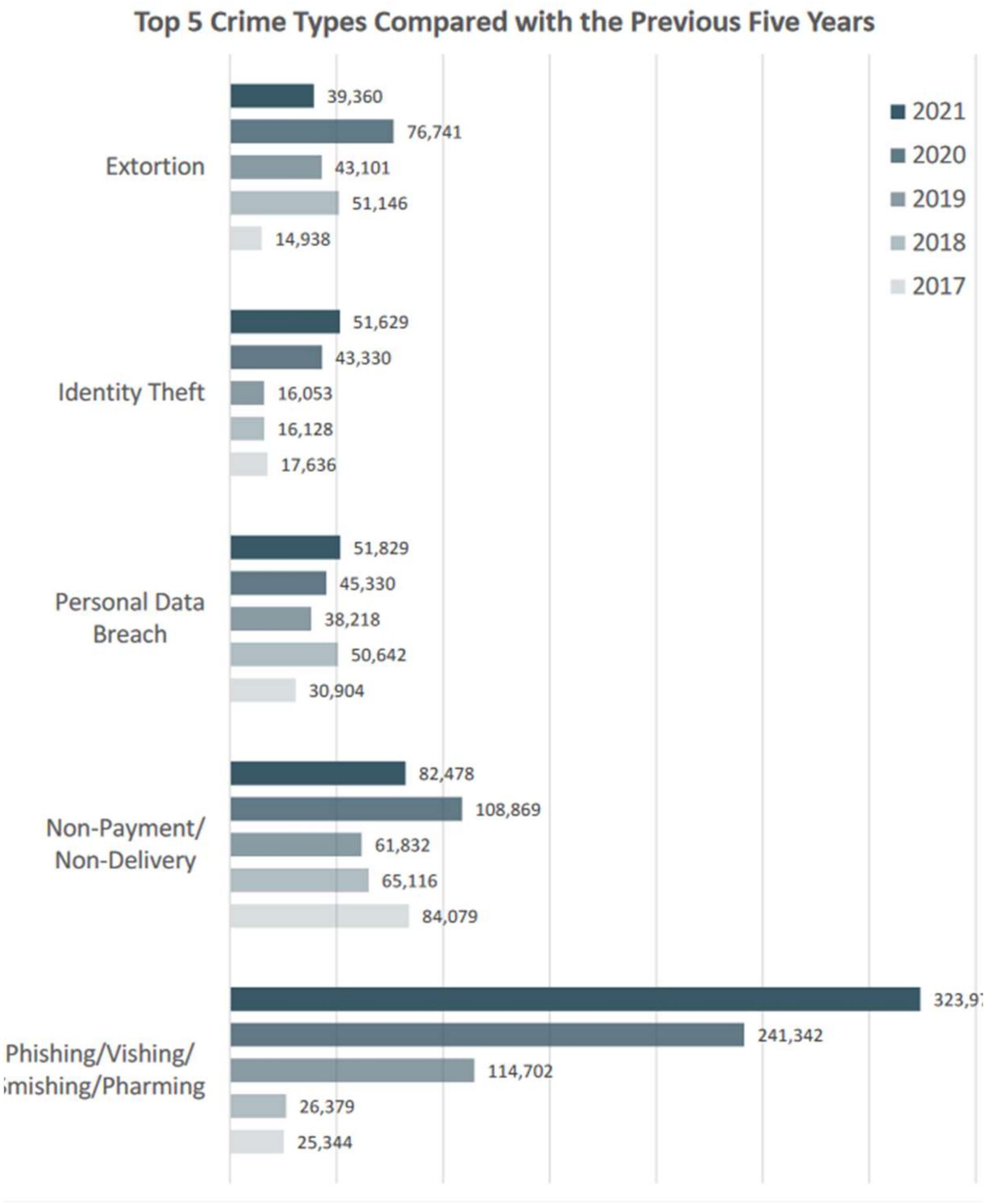
Real Estate

Scams: Rental, Timeshare, Loan Modification

IC^3 2021 Reports

Types of Crimes Reported

Top 5 crime types compared over the last 5 years



IC^3 2021 Reports
Types of Complaints

Hit Man

You get an email saying that sender has been hired to kill you unless you do something such as send money or convert to some specific religion

Ransomware *(e.g., Citadel)*

Virus that freezes your computer and states that you

Violated a law

Your IP address visited a child porno site

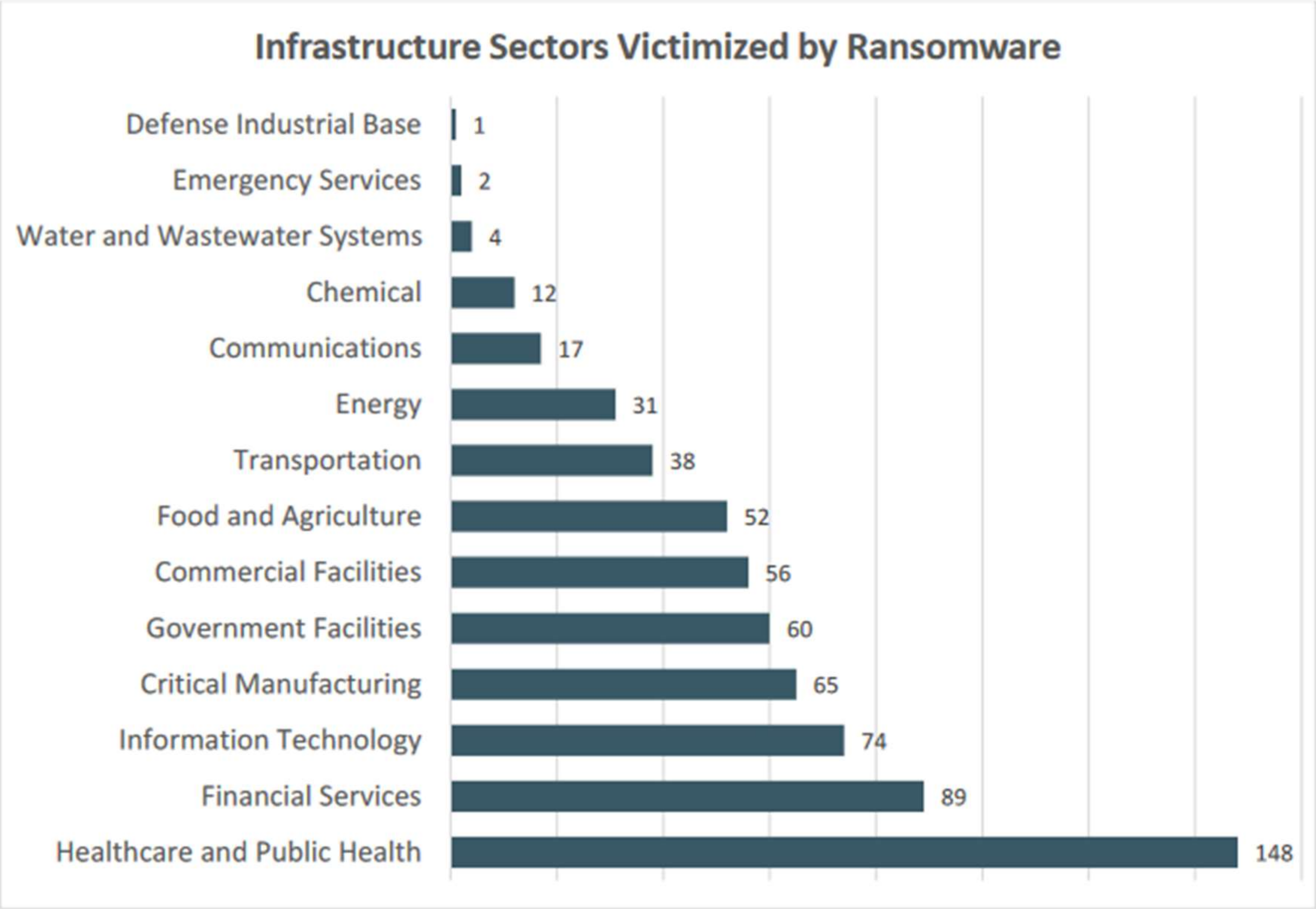
Go to DoJ web site it gives you and pay a fine

Only after you pay the fine will your computer be unfrozen

After you pay fine, virus Citadel continues to be a trojan doing online banking and credit card fraud

IC^3 2021 Reports

Ransomware



IC^3 2021 Reports
Types of Complaints

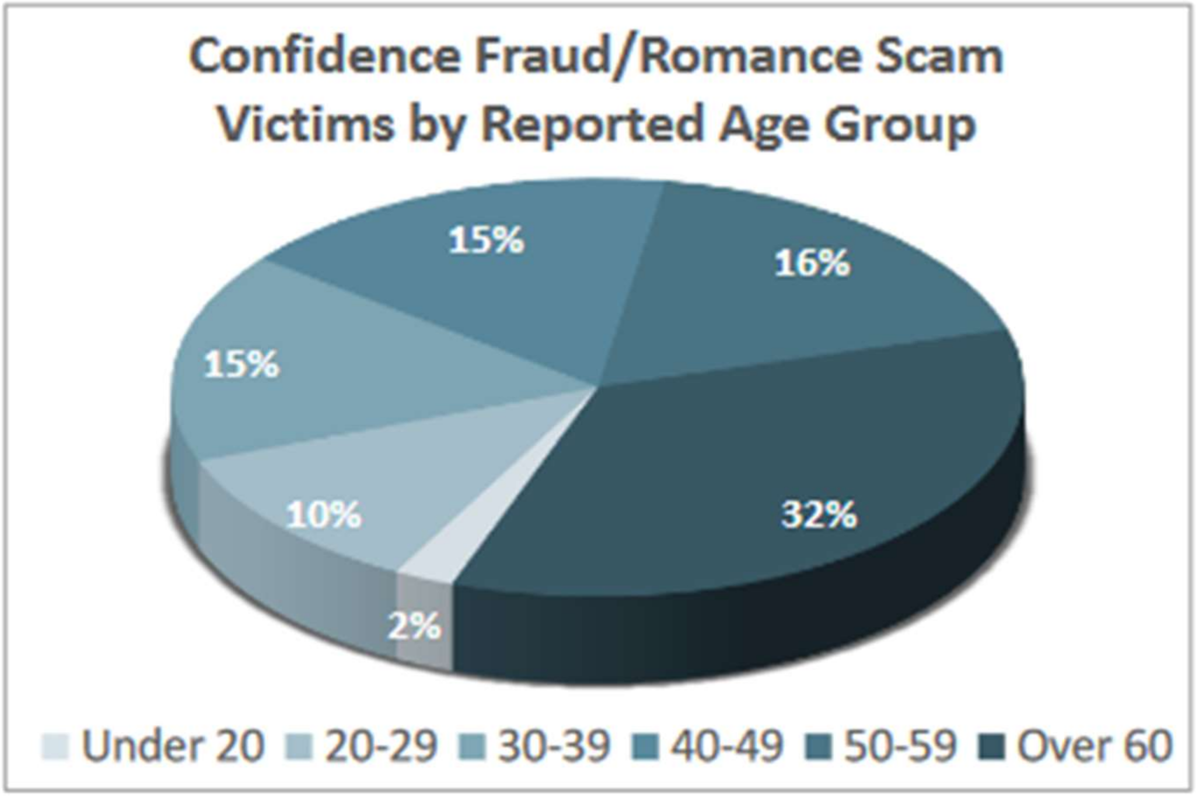
Confidence Fraud/Romance

- *Love and romance promised*
- *Perp scans and uses chat rooms, dating sites and social media sites*
- *To build trust, victim initially gets small gifts, poetry, claims of common interest or the promise of companionship*
- *Then the perp*
  - Suddenly has an emergency and needs money OR
  - Asks victim to receive packages and reship them out of country OR
  - Other activity that is likely to be nefarious

IC^3 2021 Reports *Confidence Fraud/Romance Scam*

2021 Statistics with respect to Confidence Fraud/Romance Scams:

- 24, 299 victims
- $956 million in losses
- 3rd highest losses reported by victims



IC^3 2021 Reports
Types of Complaints

Web sites with

- *Fake Designer Merchandise*
- *Low Cost versions of expensive software*
- *Ponzi schemes*

IC^3 2021 Reports
Types of Complaints

Tech Support Fraud in 2021:

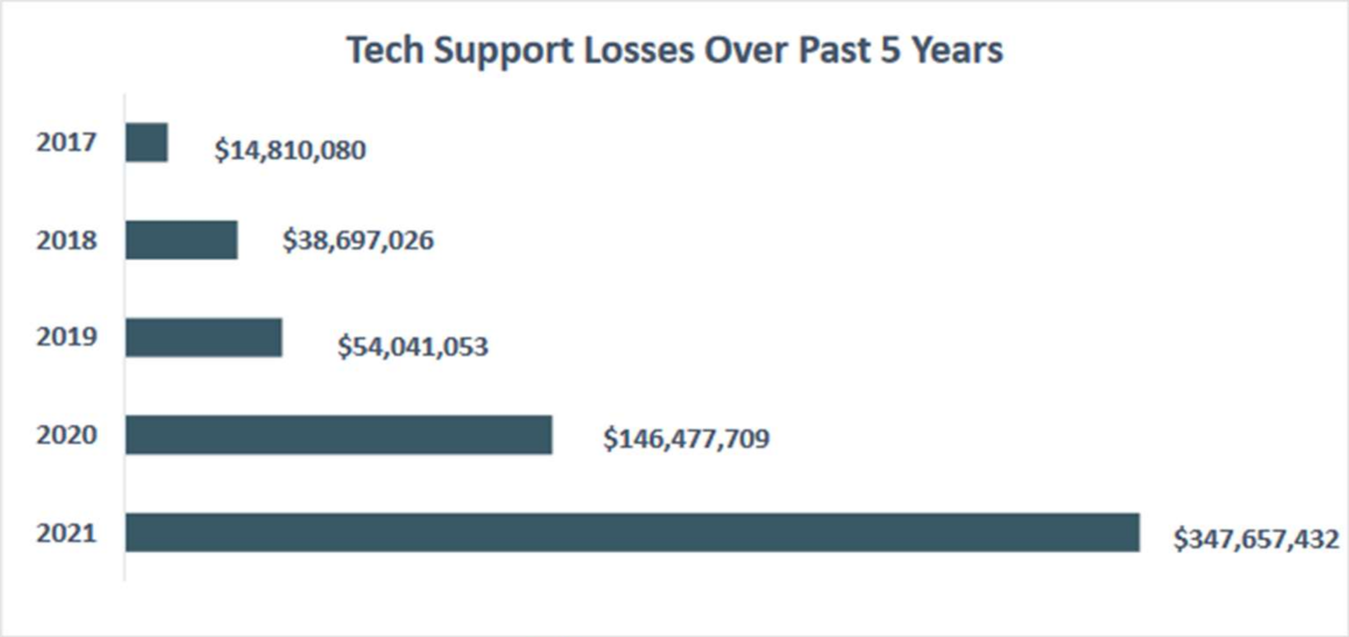
23, 903 complaints

70 countries

Losses: $347 million (37% increase over 2020)

Most victims are > 60 years old

- > 60 % of victims
- > 68% of losses

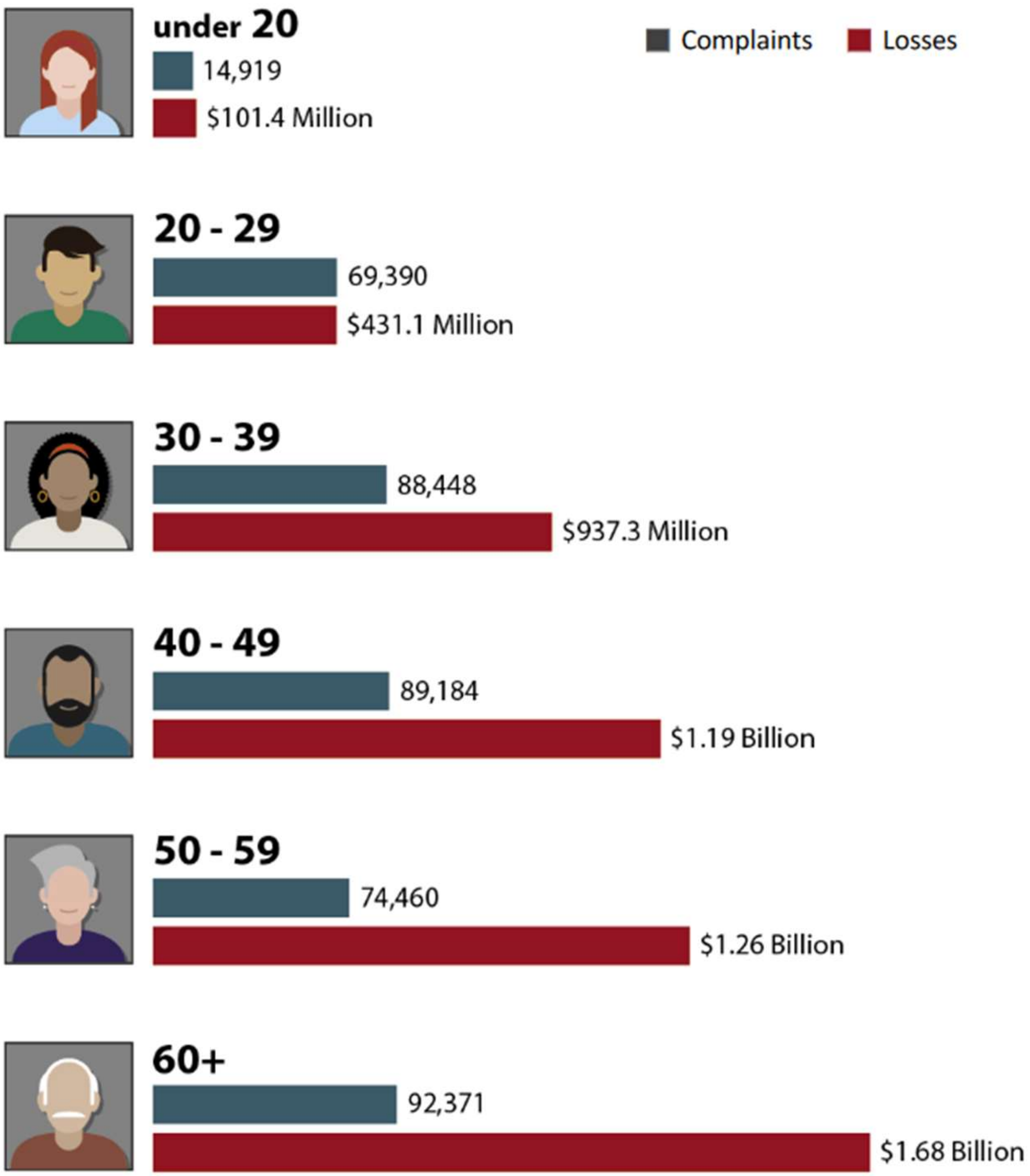


IC^3 2021 Reports
Types of Complaints

Cryptocurrency

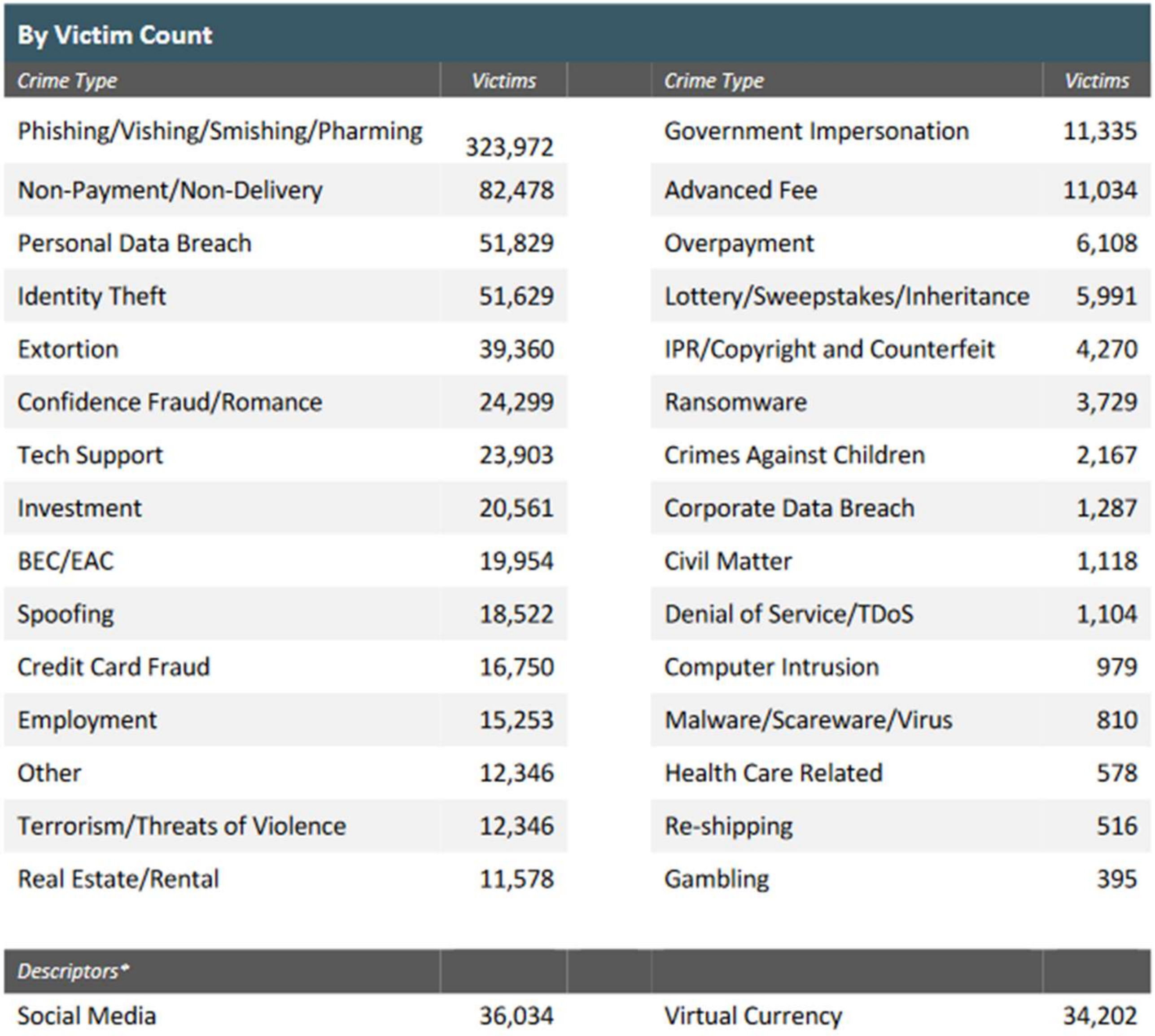
- *Number of victims decreased by more than 35,000*
- *Loss amount increased 7x (now $1.6 billion)*
  - Value of cryptocurrencies increased dramatically
  - Cryptocurrency is now being used for all types of scams
  - Especially pervasive in investment scams
    - *Losses can reach hundreds of thousands of dollars per victim*
- *Scams of note*
  - Cryptocurrency ATMs
  - Cryptocurrency support impersonators
  - Romance scams

2021 Victims by Age Group[17]



2021 IC^3 Crime Types

By Victim Count

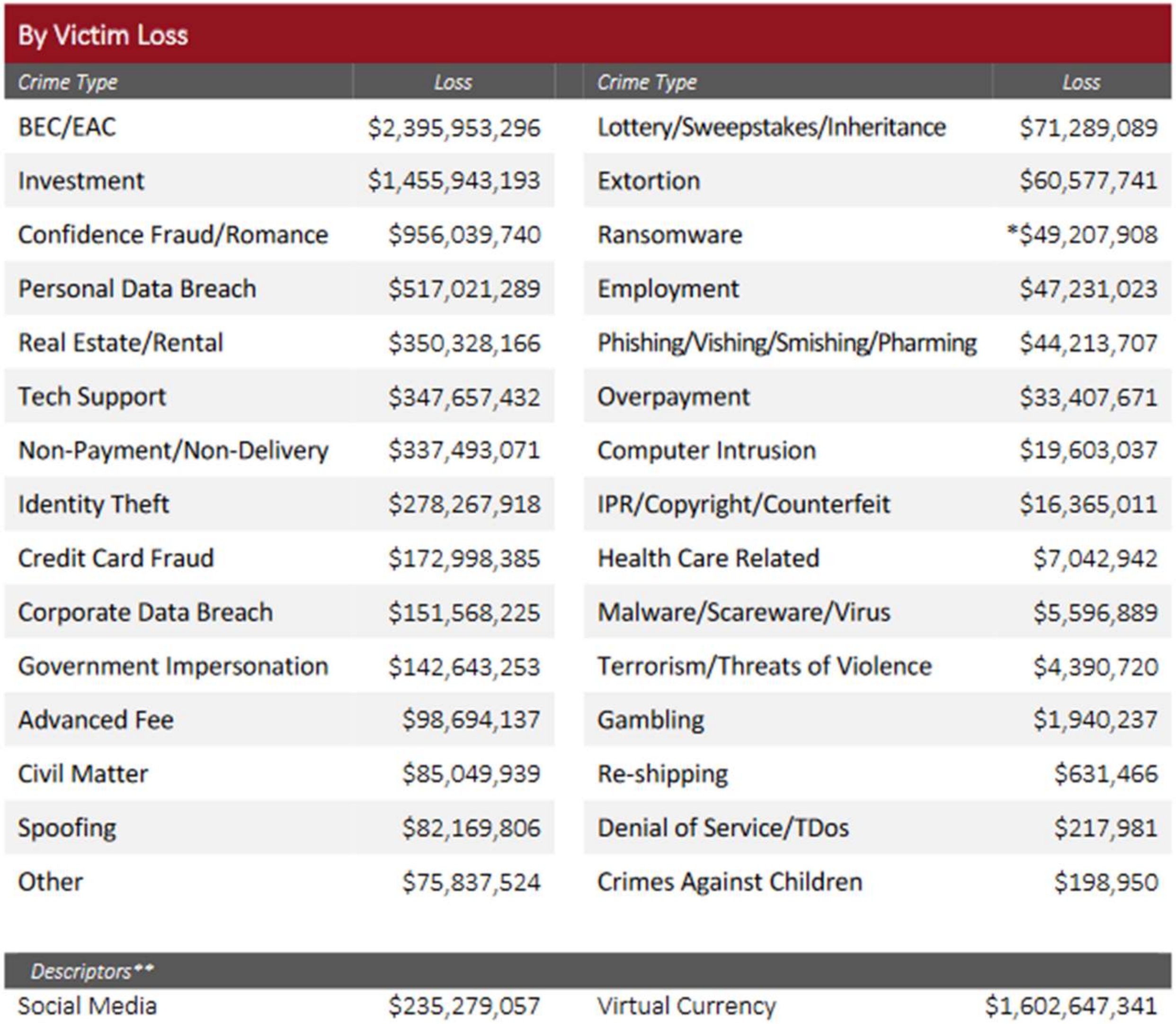


By Victim Count

Crime Type	Victims	Crime Type	Victims
Phishing/Vishing/Smishing/Pharming	323,972	Government Impersonation	11,335
Non-Payment/Non-Delivery	82,478	Advanced Fee	11,034
Personal Data Breach	51,829	Overpayment	6,108
Identity Theft	51,629	Lottery/Sweepstakes/Inheritance	5,991
Extortion	39,360	IPR/Copyright and Counterfeit	4,270
Confidence Fraud/Romance	24,299	Ransomware	3,729
Tech Support	23,903	Crimes Against Children	2,167
Investment	20,561	Corporate Data Breach	1,287
BEC/EAC	19,954	Civil Matter	1,118
Spoofing	18,522	Denial of Service/TDoS	1,104
Credit Card Fraud	16,750	Computer Intrusion	979
Employment	15,253	Malware/Scareware/Virus	810
Other	12,346	Health Care Related	578
Terrorism/Threats of Violence	12,346	Re-shipping	516
Real Estate/Rental	11,578	Gambling	395
*Descriptors**			
Social Media	36,034	Virtual Currency	34,202

2021 IC^3 Crime Types

By Victim Loss



By Victim Loss

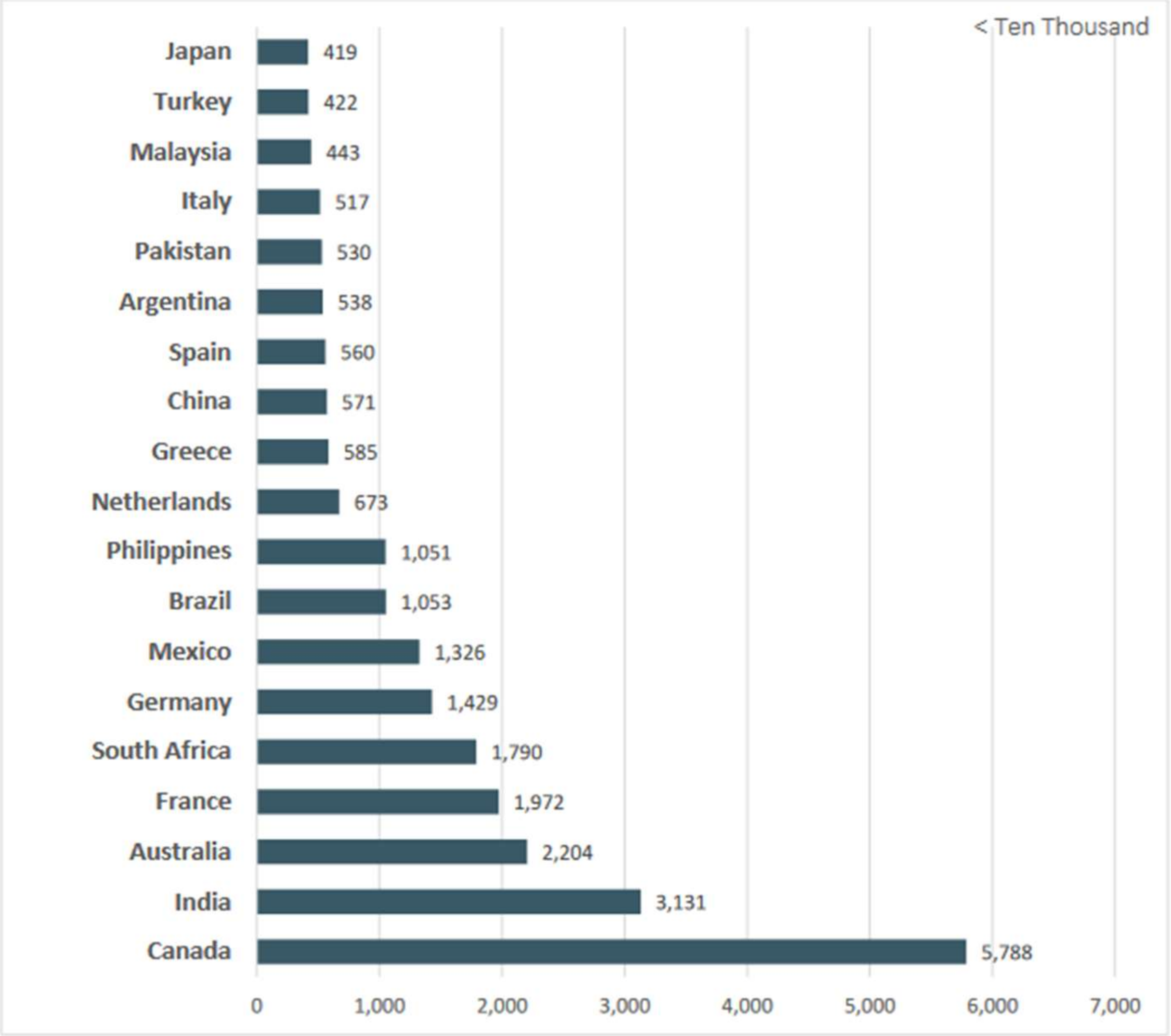
Crime Type	Loss	Crime Type	Loss
BEC/EAC	$2,395,953,296	Lottery/Sweepstakes/Inheritance	$71,289,089
Investment	$1,455,943,193	Extortion	$60,577,741
Confidence Fraud/Romance	$956,039,740	Ransomware	*$49,207,908
Personal Data Breach	$517,021,289	Employment	$47,231,023
Real Estate/Rental	$350,328,166	Phishing/Vishing/Smishing/Pharming	$44,213,707
Tech Support	$347,657,432	Overpayment	$33,407,671
Non-Payment/Non-Delivery	$337,493,071	Computer Intrusion	$19,603,037
Identity Theft	$278,267,918	IPR/Copyright/Counterfeit	$16,365,011
Credit Card Fraud	$172,998,385	Health Care Related	$7,042,942
Corporate Data Breach	$151,568,225	Malware/Scareware/Virus	$5,596,889
Government Impersonation	$142,643,253	Terrorism/Threats of Violence	$4,390,720
Advanced Fee	$98,694,137	Gambling	$1,940,237
Civil Matter	$85,049,939	Re-shipping	$631,466
Spoofing	$82,169,806	Denial of Service/TDos	$217,981
Other	$75,837,524	Crimes Against Children	$198,950

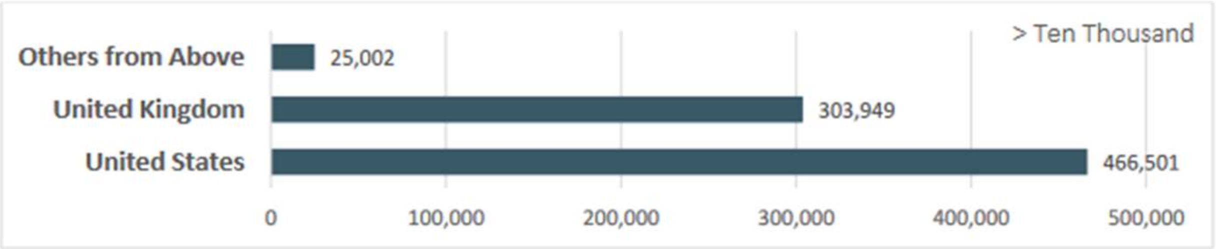
Descriptors**			
Social Media	$235,279,057	Virtual Currency	$1,602,647,341

IC^3 2021 Reports *Top 20 International Victim Countries*

Compared to the United States

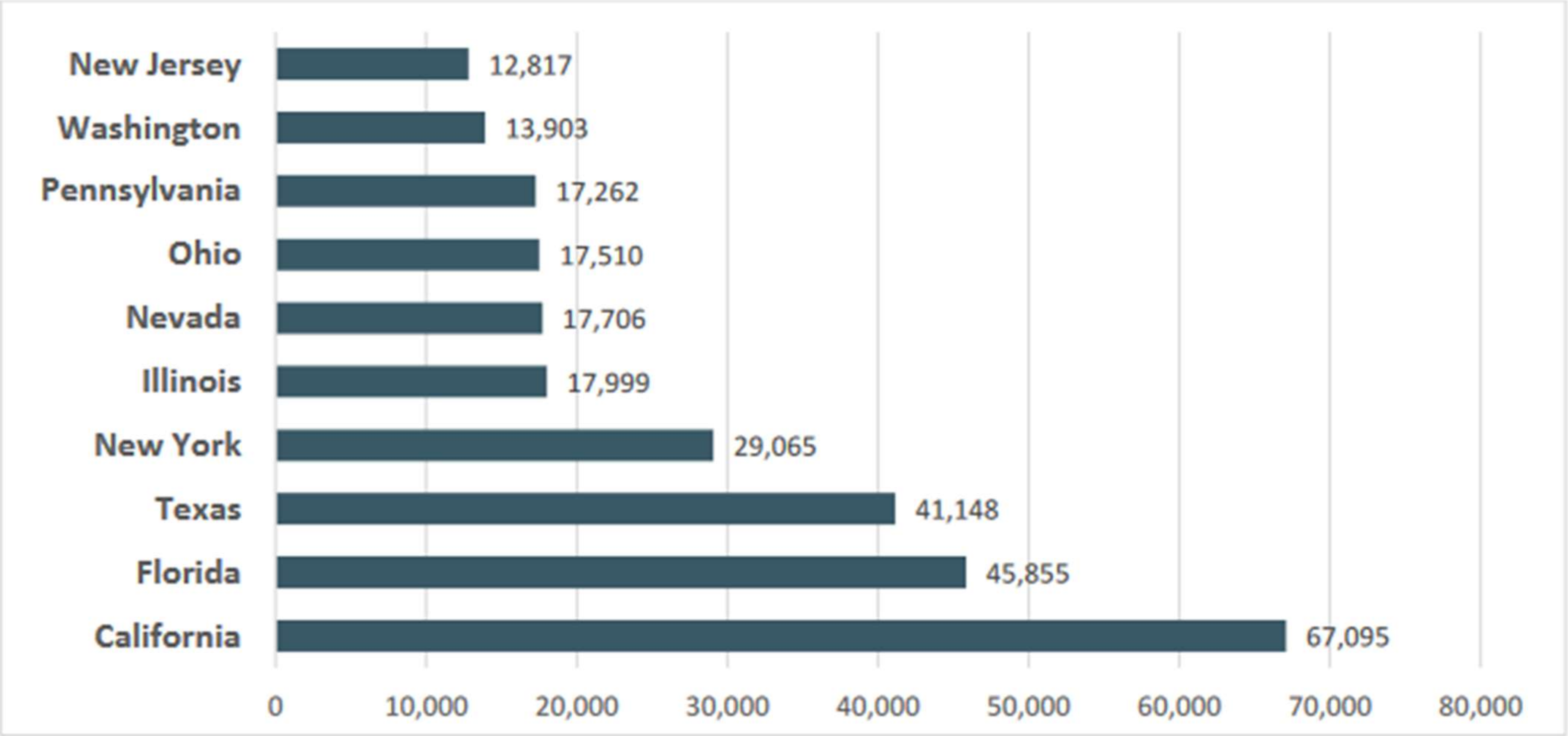
How does the US compare to the rest of the world?



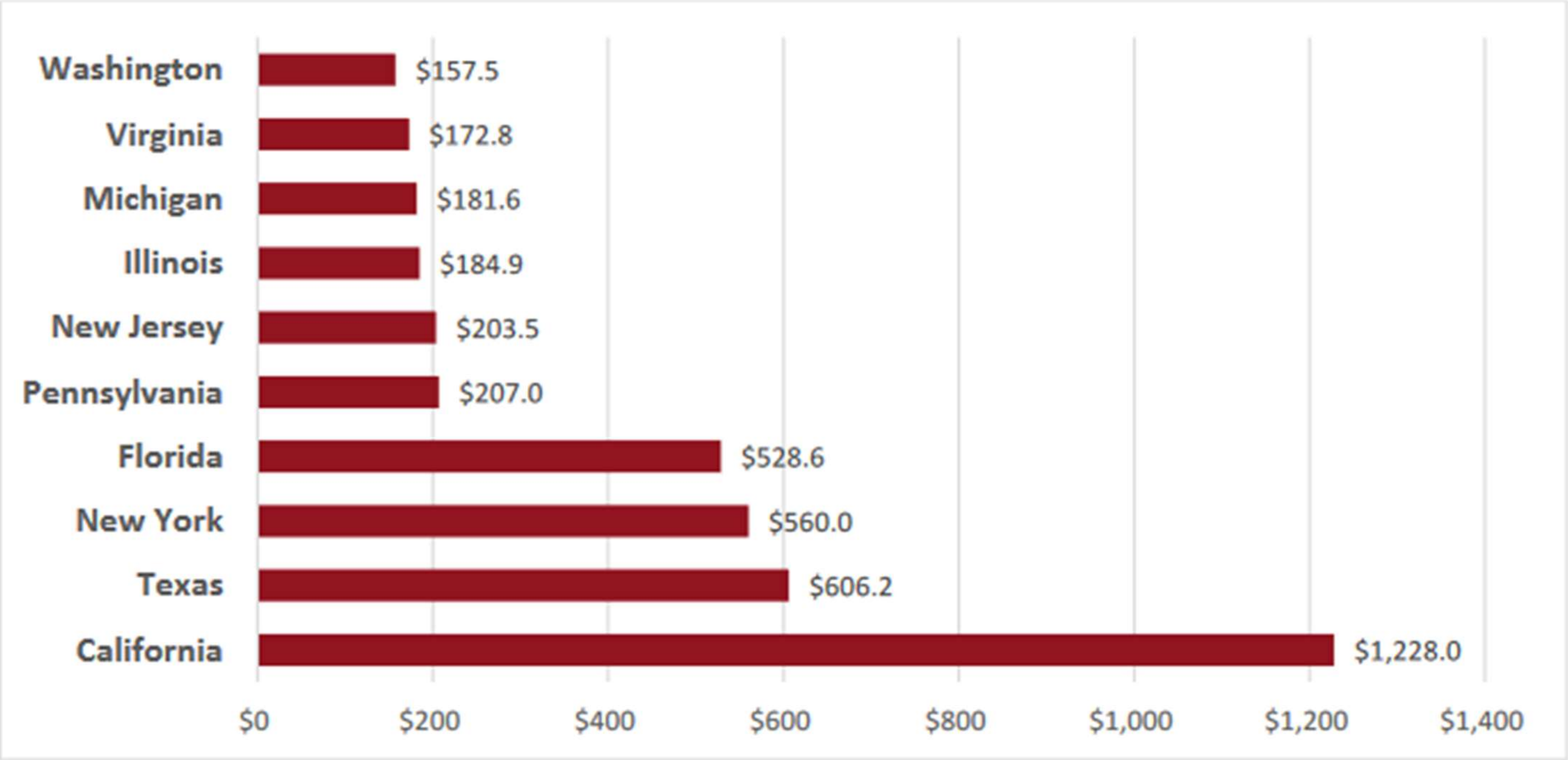


IC^3 2021 Reports

Top 10 States by # of Victims

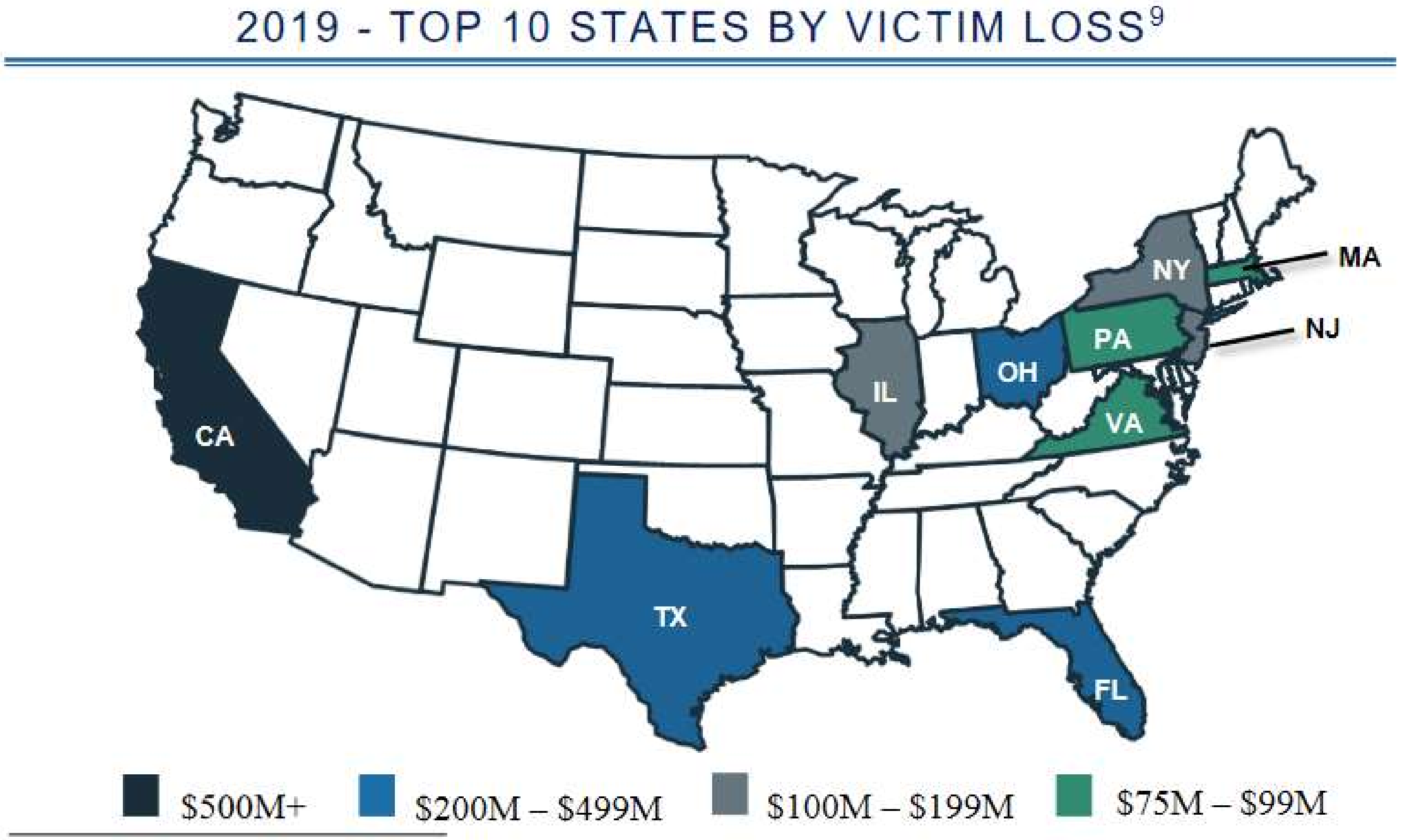


IC^3 2021 Reports
Top 10 States by Victim Loss



IC^{3} 2019 Reports

Top 10 States – by victim loss



2019 - TOP 10 STATES BY VICTIM LOSS[9]

Investigator Certification

This topic discusses a number of organizations that certify computer forensic investigators

Investigator Certification
IACIS

International Association of Computer Investigative Specialists (IACIS)

Early professional computing-forensics organization

Created by law enforcement organizations

Members who pass IACIS certification are called

Certified Forensic Computer Examiners (CFCEs)

Goal: Formalize credentials in computing investigations

www.iacis.com

Investigator Certification
IACIS

Three types of membership

- *Regular*
- *Associate*
- *Fulltime Student*

Investigator Certification

IACIS Regular Membership

Regular Membership open to

- *Present or past law enforcement personnel*
- *Government employee*
- *Current full-time forensic contractor for a gov't agency*

Cannot be a Regular Member otherwise

Full benefits

- *Training*
- *Access to experts*
- *Free annual re-certification & one-on-one peer review*
- *Can vote and hold IACIS organization offices*

Investigator Certification

IACIS Associate Membership

Associate membership open to

- *Computer Forensic Practitioners*
- *Open to anyone who can pass a background check*
- *Same as Regular members, but can't vote or hold organizational offices*

Benefits

- *Similar to Regular membership*

Investigator Certification

IACIS Student Membership

Student membership open to

- *Full-time Students enrolled in accredited school*

Benefits

- *Similar to Associate membership*

Investigator Certification
IACIS Training

Basic Computer Forensic Examiner (BCFE) Course

- *Covers many of the things that you will get in this course*
- *Two-consecutive-week in-person course*
- *No prerequisite knowledge*
- *Costly, but you get a computer, write blocker, external hard drive and other stuff.*

Investigator Certification
IACIS Training

Certified Incident Forensics Response (CFIR)

- *Peer review*
- *Prerequisite: The BCFE Course*
- *Exam (includes both practicum and written)*

Re-certification

- *Must re-certify every three years*
- *Keep up with technology changes*

Investigator Certification

Other IACIS Training

ACF: Applied Computer Forensics

BCFE: Basic Computer Forensic Examiner

CIFR: Cyber Incident Forensic Response

Digital Forensics Using Open Source Tools

Mac I: Best Practices in Mac Forensics

Mac II: Advanced Practices in Mac Forensics

Managing a Digital Forensics Lab

MDF: Mobile Device Forensics

PLA: Preparing for Lab Accreditation

RAM Capture and Analysis

SVR: Surveillance Video Recovery

WFE: Windows Forensic Examiner

Investigator Certification
HTCN Training & Certification

High Tech Crime Network (HTCN)

Provides certification for computer crime investigators and computing-forensics technicians

Has four different certifications

Crime Investigator basic	*Crime Investigator advanced*
Forensic Technician basic	*Forensic Technician advanced*

Membership <u>not</u> restricted

Low cost student memberships available

www.htcn.org

Investigator Certification
HTCN Training & Certification

Certified Computer Crime Investigator, Basic

- *3 years of law-enforcement or corporate investigative experience*
- *40 hours of training from approved agency, organization or training company*
- *10 or more documented cases in which candidate participated*

Certified Computer Crime Investigator, Advanced

- *5 years of investigative experience in any area*
- *80 hours of related training from an approved source*
- *Must have served as lead investigator in at least 20 cases and were involved with at least 40 cases as a lead investigator, supervisor, or in a supportive capacity.*
- *Total case involvement must be 60 or more*

Investigator Certification
HTCN Training & Certification

Certified Computer Forensic Technician Basic

Same requirements for Certified Computer Crime Investigator Basic, but all experience must be related to computer forensics

Certified Computer Forensic Technician Advanced

Same requirements for Certified Computer Crime Investigator Advanced, but all experience must be related to computer forensics

Some approved sources of training are on their web site

Investigator Certification

Some Other Training & Certification

Access Data Certified Examiner

- *Trains on use of* **Access Data** *products*
- *Do not need to take Access Data training, but must demonstrate that you can use it in order to be certified*

EnCase Certified Examiner

- *EnCE: EnCase Certified Examiner*
- *Trains on use of* **EnCase** *software*
- *Do not need to take EnCase training, but must demonstrate that you can use it in order to be certified*

Investigator Certification

Some Other Training & Certification

EC-Council

www.eccouncil.org

SysAdmin, Audit, Network, Security Institute (SANS)

digital-forensics.sans.org/certification

Computer Technology Investigators Network (CTIN)

www.ctin.org

High Technology Crime Investigations Assoc. (HTCIA)

www.htcia.org

International Society of Forensic Computer Examiners (ISFCE)

www.isfce.com

Digital Forensics Certification Board (DFCB)

www.dfcb.org/certification.html

Certified Cyber Forensics Professional

www.isc2.org/ccfp/default.aspx

Investigator Certification

Some Other Training & Certification

Federal Law Enforcement Training Center (FLETC)

- *www.fletc.gov*
- *Now part of Homeland Security*

National White Collar Crime Center (NW3C)

- *www.nw3c.org*