

Snapshot: IC3 Cyber Crime Statistics in 2024

Prepared by **HexForensic.com**

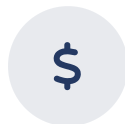


HexForensic.com



859,532

Total Complaints



\$16.6 Billion

Total Financial Losses



33%

Increase in Losses from 2023



256,256

Complaints Reporting Financial Loss



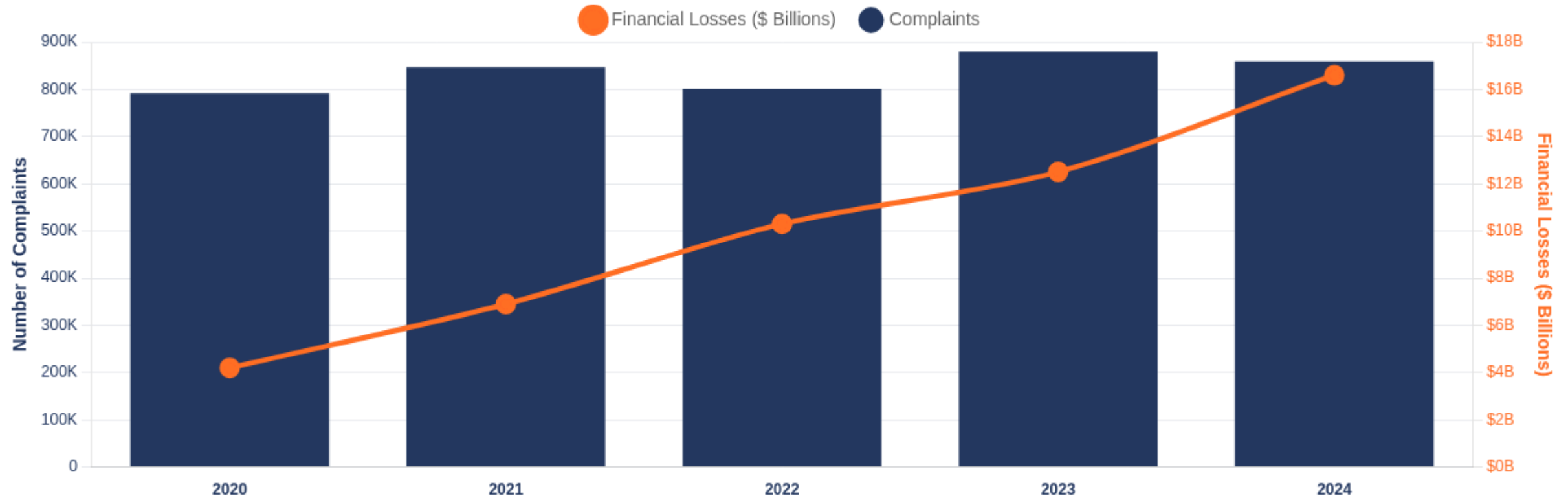
\$19,372

Average Financial Loss per Complaint

In 2024, the FBI's Internet Crime Complaint Center (IC3) was inundated with **859,532 complaints**, culminating in staggering reported financial losses of **\$16.6 billion**. This marks a disturbing **33% escalation** in losses compared to the preceding year. Of these, **256,256 complaints** involved direct financial repercussions, with victims losing an average of **\$19,372** per incident that resulted in a monetary loss.



Five-Year Trend: IC3 Complaints + Financial Losses (2020-2024)



4.2 Million

Total Complaints (2020-2024)

\$50.5 Billion

Total Financial Losses (2020-2024)

Analyzing the trajectory from 2020 to 2024, while complaint numbers have seen some fluctuation, peaking in 2023, the financial toll of these cybercrimes has climbed **relentlessly and alarmingly**. Reported losses surged from approximately \$4.2 billion in 2020 to a stark \$16.6 billion in 2024. Cumulatively, over these five years, the IC3 processed **4.2 million complaints**, corresponding to a monumental **\$50.5 billion** in documented losses, underscoring the escalating proficiency and impact of cybercriminals.

Victim Demographics: 2024 Segmented by Age



HexForensic.com



A demographic breakdown of victims reveals that individuals aged **60 and over** were the most targeted, lodging the highest number of complaints (**147,127**) and enduring the most substantial financial setbacks, totaling **\$4.8 billion** in losses in 2024. Although the 40-49 age group also registered a high complaint volume (112,755), their financial losses were less than half of those borne by the elderly population, pointing to a significant vulnerability among seniors.

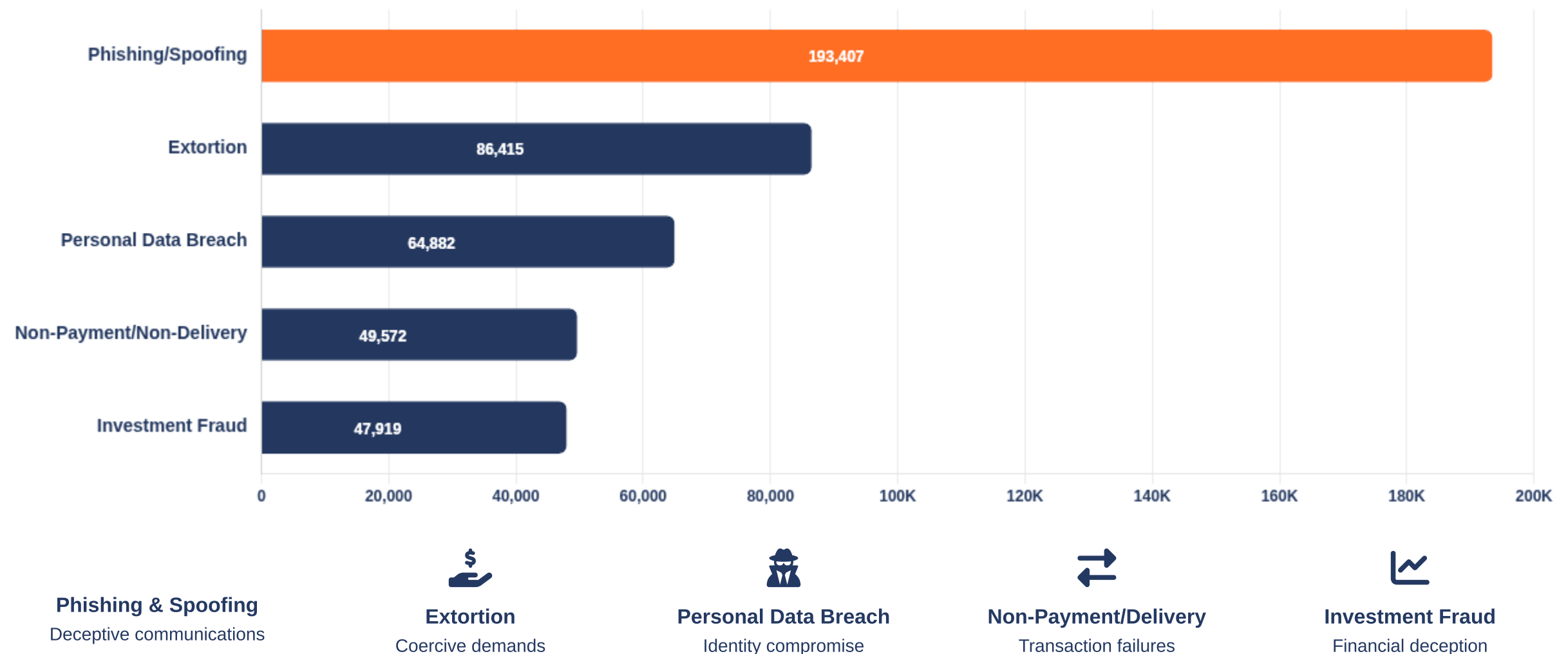
💡 KEY INSIGHT

While those 60+ represent only 17% of all complaints, they account for nearly 29% of all financial losses.

Anatomy of Cybercrime: Top 5 Crime Categories by Complaint Volume



Most frequently reported cyber crime types to IC3 in 2024



By sheer frequency, **Phishing and Spoofing** attacks dominated the reports in 2024, with **193,407 complaints** filed. These were followed in volume by Extortion schemes (86,415 complaints) and incidents of Personal Data Breach (64,882 complaints). This indicates that deceptive tactics aimed at illicit information gathering and coercive threats remain the most common tools in the cybercriminal arsenal.

KEY INSIGHT

Phishing/Spoofing complaints exceeded the next highest category (Extortion) by **124%**, highlighting the overwhelming prevalence of social engineering tactics.

Financial Impact: Top 5 Crime Categories by Reported Losses



Most financially devastating cyber crime types in 2024



When assessing the financial devastation, **Investment fraud** emerged as the costliest crime category, siphoning over **\$6.57 billion** from victims. Business Email Compromise (BEC) ranked second, with losses exceeding **\$2.77 billion**, while Tech Support scams also led to significant financial damage, surpassing **\$1.46 billion**. This disparity shows that while some crime types are more frequent, others are vastly more profitable for perpetrators.

FREQUENCY vs. IMPACT

Investment fraud ranks 5th in complaint volume but 1st in financial losses, demonstrating its outsized financial impact.

Deep Dive: Cyber-Enabled Fraud Landscape in 2024



Where technology is the primary instrument for financial deception

333,981

TOTAL FRAUD COMPLAINTS

\$13.7B

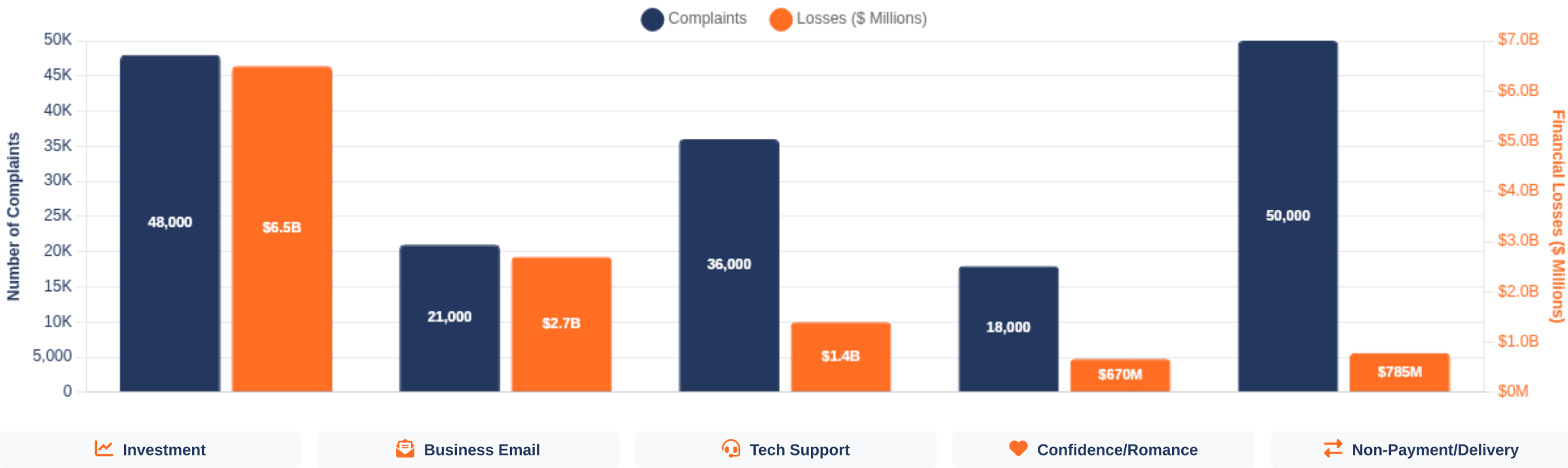
TOTAL FRAUD LOSSES

38%

OF ALL 2024 COMPLAINTS

83%

OF ALL 2024 FINANCIAL LOSSES



Cyber-enabled fraud – where technology is the primary instrument for deceit – continues to be a dominant concern. In 2024, these fraud types constituted **333,981 complaints** (making up **38%** of all reports) and resulted in an overwhelming **\$13.7 billion** in losses, which is **83%** of the total financial damage reported to IC3. Within this category, **Investment scams**, **Business Email Compromise**, and **Tech Support fraud** were the primary drivers of these extensive financial losses.

Focus: Cyber Threats Targeting Critical Infrastructure



Ransomware and Data Breach incidents across vital sectors in 2024



263,455

TOTAL CYBER THREAT COMPLAINTS



\$1.571 Billion

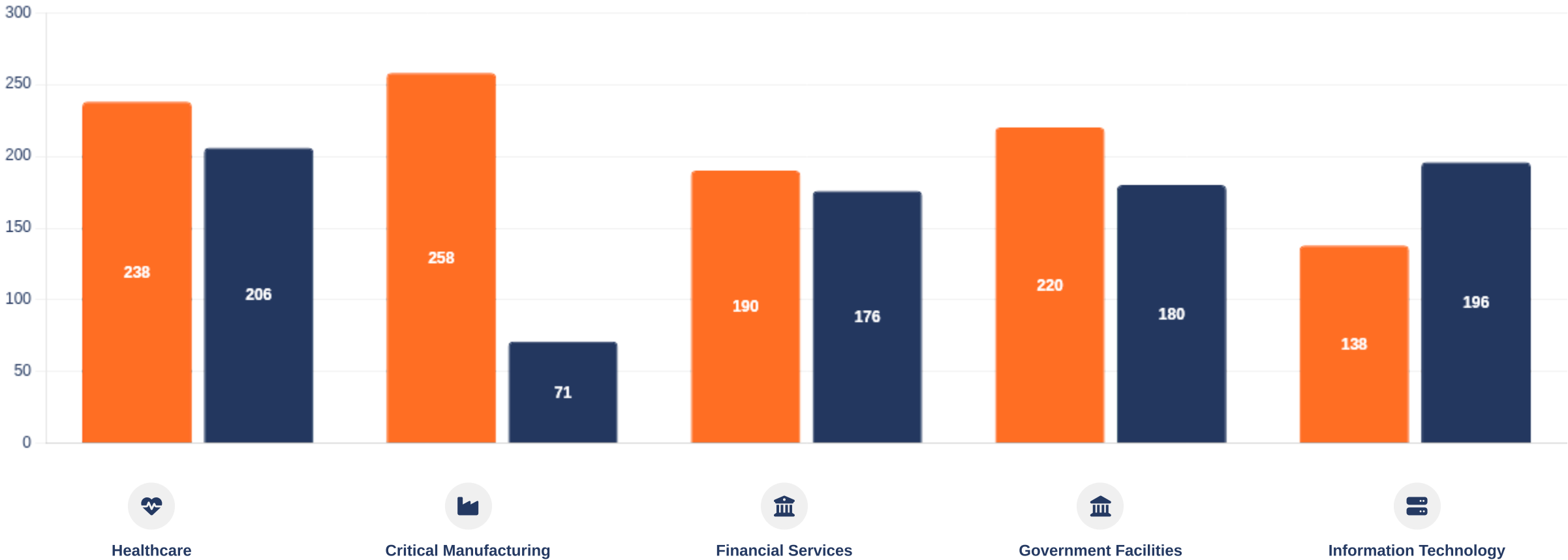
TOTAL LOSSES FROM CYBER THREATS



4,878

COMPLAINTS FROM CRITICAL INFRASTRUCTURE SECTORS

 Ransomware  Data Breach



Direct cyber threats, including ransomware and data breaches, also present a substantial risk, with IC3 registering **263,455 such complaints** leading to over **\$1.57 billion** in losses in 2024. Attacks against critical infrastructure are particularly alarming, with **4,878 incidents** reported from these vital sectors. The **Healthcare/Public Health** and **Critical Manufacturing** sectors were among the hardest hit, reporting high instances of both ransomware and data breaches, underscoring their susceptibility to these crippling attacks.

Intervention Success: Financial Fraud Kill Chain (FFKC) Impact



Preventing fraudulent transfers through rapid response in 2024



3,020

COMPLAINTS REFERRED TO FFKC



\$848.4 Million

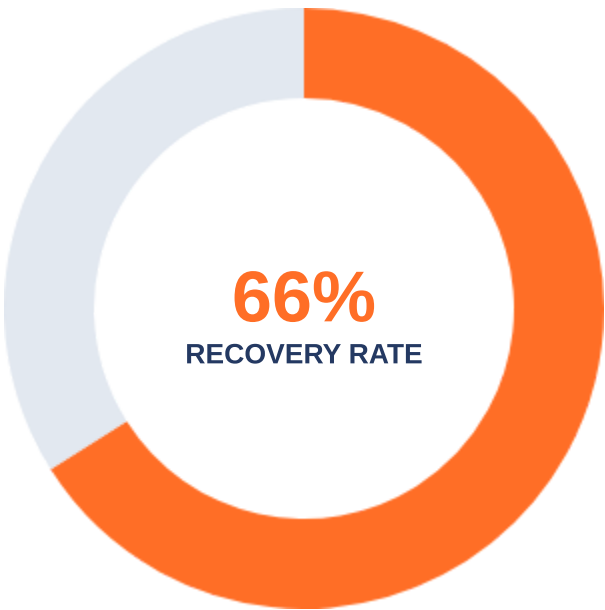
TOTAL ATTEMPTED THEFT VALUE



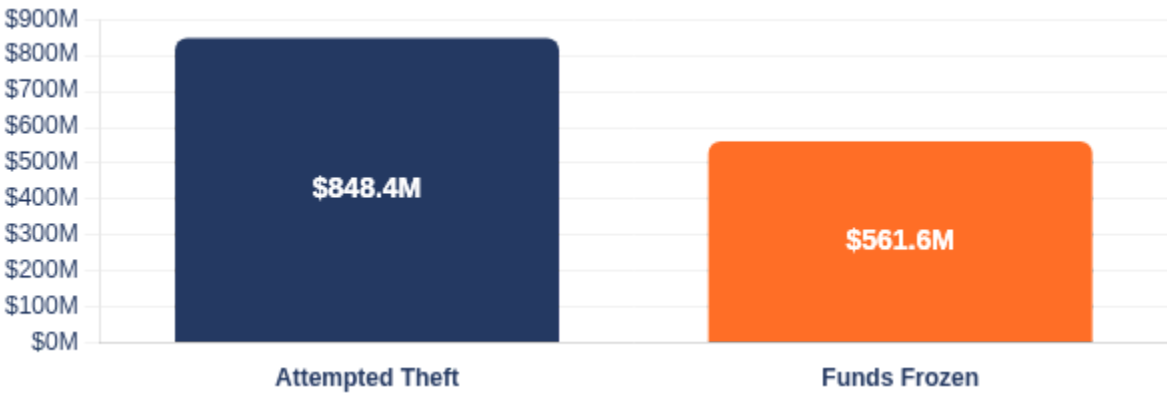
\$561.6 Million

TOTAL VALUE OF FUNDS FROZEN

FFKC Success Rate



Funds Breakdown (in Millions)



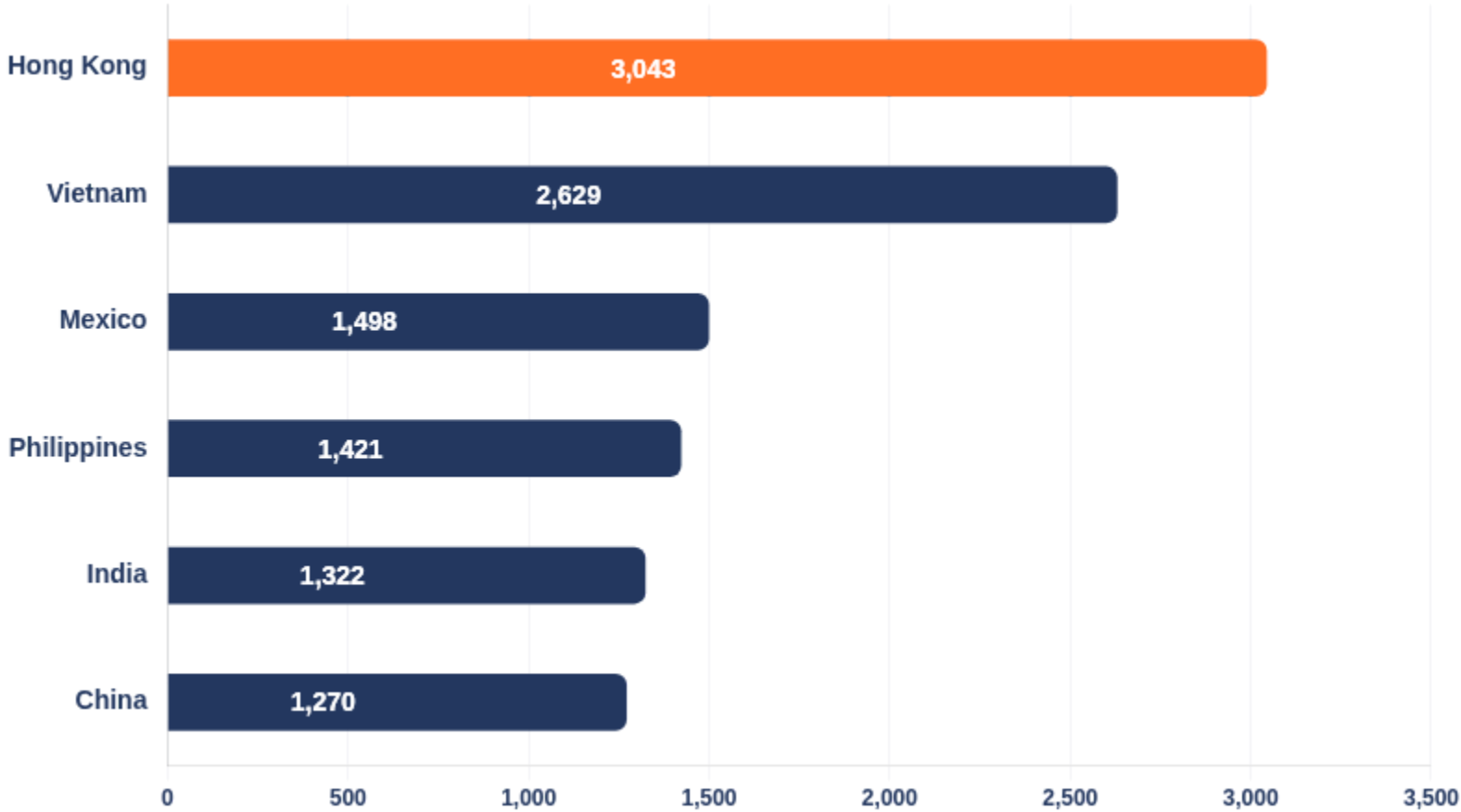
Frozen Funds Origin

- Domestic \$469.1M (84%)
- International \$92.5M (16%)







The IC3's Recovery Asset Team (RAT) is instrumental in mitigating losses via the Financial Fraud Kill Chain (FFKC). In 2024, the FFKC was activated for **3,020 complaints** involving attempted thefts totaling **\$848.4 million**. Proactive measures led to the freezing of **\$561.6 million** (\$469.1 million domestically and \$92.5 million internationally), achieving a significant **66% success rate** in halting reported fraudulent transactions.

Global Reach: Top International Destinations for Fraudulent Wire Transfers

Where cybercriminal proceeds were sent in 2024



Top Destinations by Transaction Count

	Hong Kong	3,043
	Vietnam	2,629
	Mexico	1,498
	Philippines	1,421
	India	1,322
	China	1,270

i Transactions represent individual fraudulent wire transfers reported to IC3.

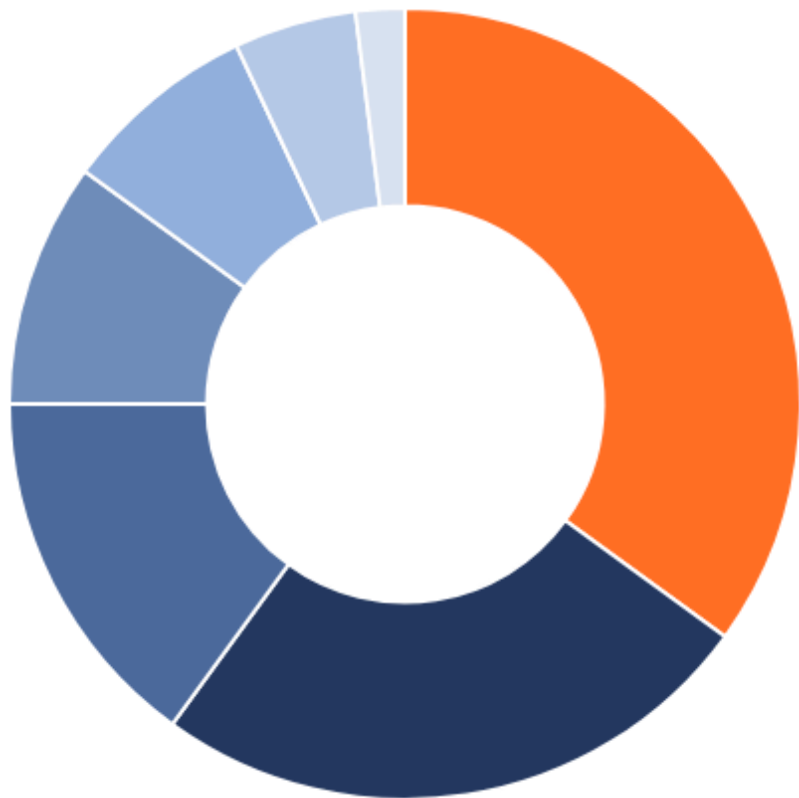
KEY INSIGHT

The top 6 international destinations received over **11,000 fraudulent transfers**, with Asia being the dominant region, receiving 73% of these transactions.

The international scope of cybercrime is evident in the destinations of illicit funds. **Hong Kong** topped the list in 2024 as the primary international destination for fraudulent wire transfers, with **3,043** such transactions reported. **Vietnam**, **Mexico**, and the **Philippines** also figured prominently as conduits for these illegally obtained funds.

Mechanisms of Loss: Predominant Transaction Methods in Fraud

Payment methods exploited by cybercriminals in 2024



KEY INSIGHT

The rise of **cryptocurrency** as the leading fraud payment method represents a significant shift from traditional banking instruments, complicating recovery efforts due to its pseudonymous nature and irreversible transactions.



Cryptocurrency
Highest risk



Wire Transfer/ACH
Second highest



Debit/Credit Card
Third highest



Peer-to-Peer Transfer
Growing risk



Gift/Prepaid Card
Medium risk



Check/Cashier's Check
Lower risk



Cash
Lowest prevalence

Understanding the methods by which victims lose money is crucial for prevention. In 2024, **cryptocurrency** emerged as the leading mechanism for financial loss in reported fraud cases, followed by **wire transfers/ACH** payments, and then **debit/credit card** fraud. This underscores the growing exploitation of digital currencies in fraudulent activities.



Elder Fraud Spotlight: Victims Aged 60+ Statistics and Trends



A disturbing pattern of exploitation targeting older Americans in 2024

147,127

TOTAL COMPLAINTS FROM 60+ AGE GROUP

↑ 46% from 2023

\$4.89 Billion

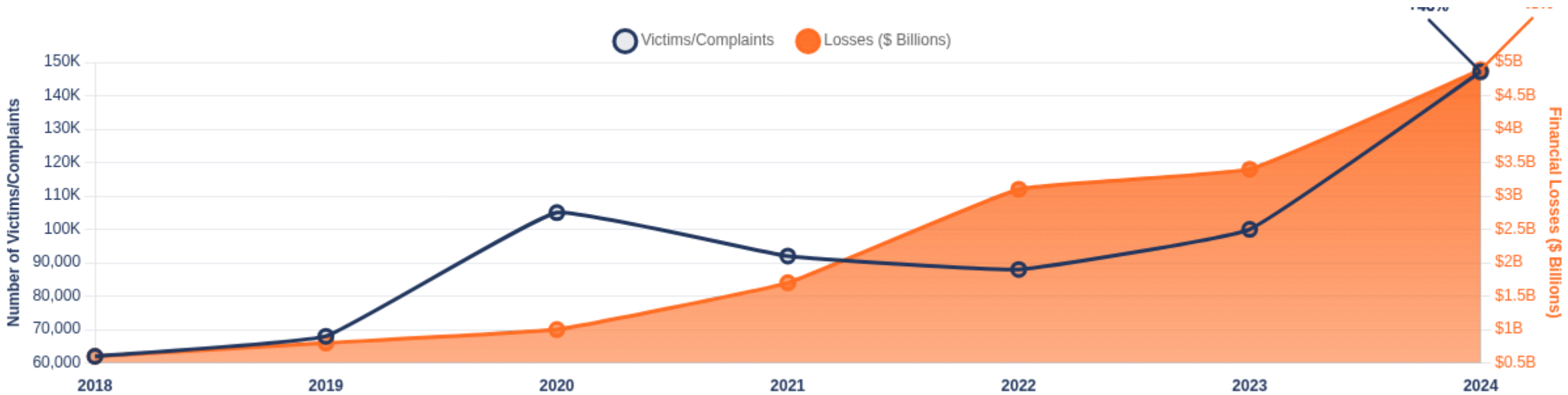
TOTAL LOSSES FOR 60+ AGE GROUP

↑ 43% from 2023

\$83,000

AVERAGE LOSS PER VICTIM

7,500 victims lost over \$100K



Individuals aged 60 and older remain a **significantly vulnerable group**. In 2024, this demographic accounted for 147,127 complaints, a sharp **46% rise** from 2023, with associated losses climbing to nearly **\$4.9 billion**—a 43% increase from the previous year. Disturbingly, **7,500 complainants** in this age bracket each lost over \$100,000, with the average loss standing at **\$83,000**. The trend data reveals a worrying escalation in both the number of elderly victims and their financial losses, especially in the most recent years.

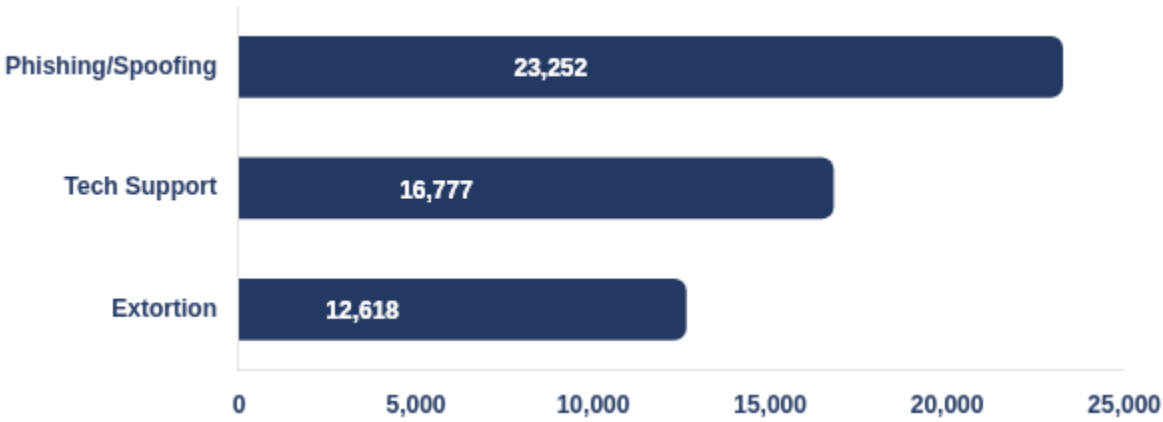
ALERT: Elder fraud is growing at an **accelerating rate** - 2024 saw the steepest increase in both victims and losses since reporting began.

Elder Fraud Deep Dive: Top Crime Types Affecting Individuals 60+

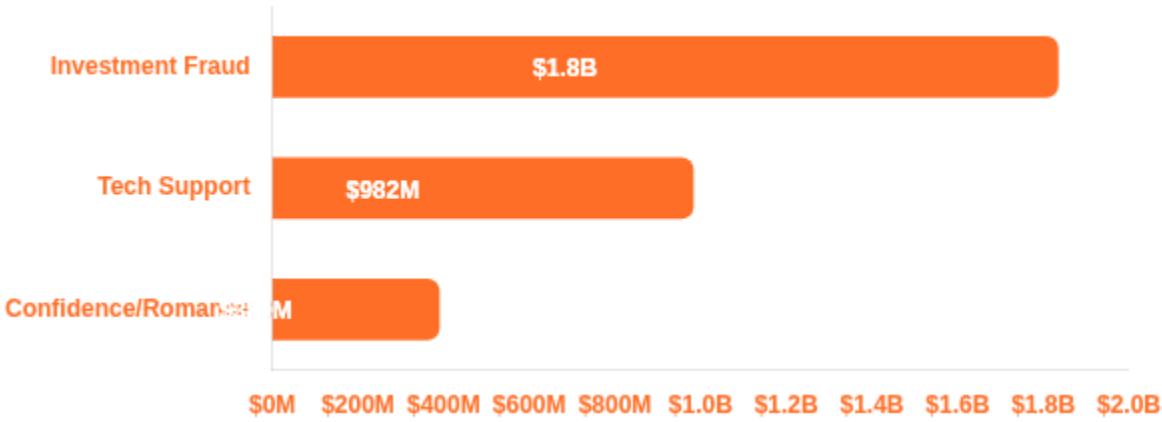


Analysis of top fraud categories targeting seniors by complaint frequency and financial impact

TOP CRIME TYPES BY COMPLAINT COUNT



\$ TOP CRIME TYPES BY FINANCIAL LOSS



Phishing/Spoofing

Deceptive emails, texts & calls designed to steal personal information

23,252

Tech Support

Fraudulent computer repair services & fake security warnings

16,777

Extortion

Threats & demands to extract money from victims

12,618

Investment Fraud

Fake investment opportunities targeting retirement accounts

\$1.83B

Tech Support Fraud

Elderly victims pay for unnecessary services & remote access

\$982M

Confidence/Romance

Relationship-based scams targeting lonely seniors

\$389M

For victims aged 60 and over, **Phishing/Spoofing** was the most frequently reported crime by count (**23,252 instances**), with **Tech Support** scams following closely (**16,777 complaints**). However, in terms of sheer financial devastation for this group, **Investment fraud** was the primary culprit, leading to losses exceeding **billion**. Tech Support scams also inflicted nearly **\$1 billion** in losses. **Confidence/Romance scams** further compounded the financial hardship faced by this vulnerable demographic.

Cryptocurrency Fraud: 2024 Overview and Alarming Trends



Analysis of the explosive growth in cryptocurrency-related fraud (2017-2024)



149,686

TOTAL COMPLAINTS REFERENCING
CRYPTOCURRENCY



\$9.3 Billion

TOTAL LOSSES FROM CRYPTO FRAUD

↑ 66%



60+ Age Group

MOST VULNERABLE DEMOGRAPHIC

33,369

Complaints

\$2.84B

Losses



Cryptocurrency-related fraud is exhibiting a **dramatic and concerning upward trend**. In 2024, the IC3 received **149,686 complaints** involving cryptocurrency, with reported losses surging to an unprecedented **\$9.3 billion** – a **66% increase** from 2023 alone. The 60+ age group bore the brunt of these scams, both in complaint volume and financial impact. The trend since 2021 clearly indicates an **exponential rise** in losses tied to cryptocurrency fraud.

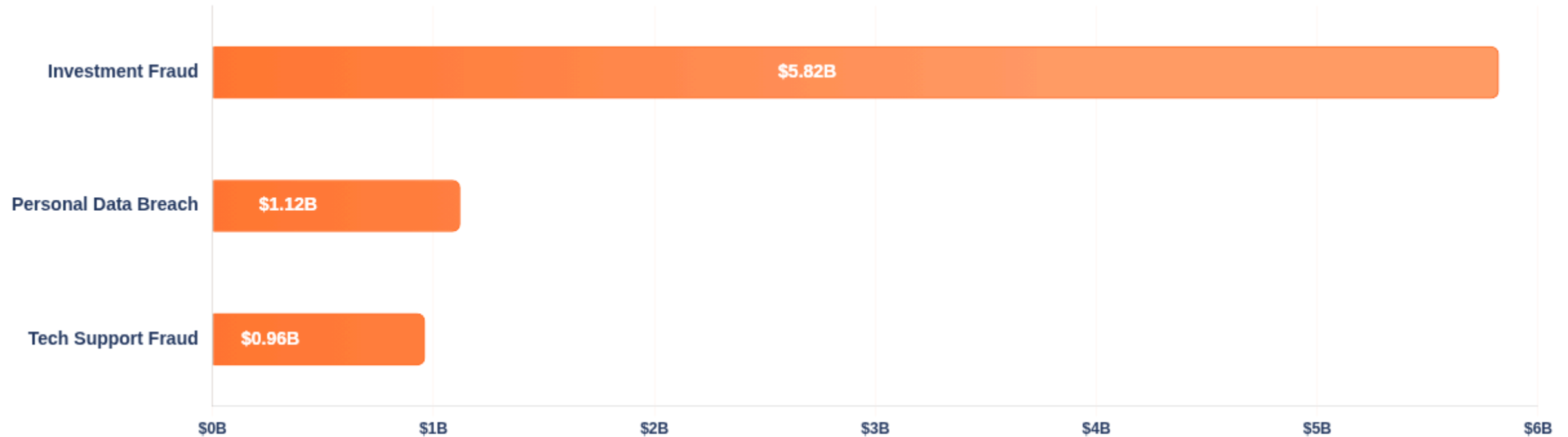


CRITICAL ALERT: Cryptocurrency losses have increased by **over 2,225%** since 2017 (\$0.4B → \$9.3B), making it the fastest-growing fraud vector in the IC3 report's history.

Cryptocurrency's Role: Top Crime Types by Loss



Where digital currencies are the preferred payment method for cybercriminals



Investment Fraud

\$5.82 Billion

Fraudulent investment schemes that exploit the complex and technical nature of cryptocurrency to deceive victims, often promising unrealistic returns.



Personal Data Breach

\$1.12 Billion

Unauthorized access to personal information, leading to cryptocurrency wallet compromises and theft of digital assets.



Tech Support Fraud

\$962 Million

Scammers pose as technical support representatives to gain access to victims' devices and cryptocurrency wallets or convince them to transfer funds.



KEY INSIGHT

Investment fraud accounts for **62%** of all cryptocurrency-related losses, demonstrating how cybercriminals exploit the speculative nature and technical complexity of cryptocurrency to defraud victims. The combined losses from these top three crime types total **\$7.9 billion**, representing 85% of all cryptocurrency-related losses reported to IC3 in 2024.