Internet Fraud Complaint Center (IFCC)

Six-Month Data Trends Report

May—November 2000

Prepared by the
National White Collar Crime Center
and the Federal Bureau of Investigation

Contents

The Internet Fraud Complaint Center
Six-Month Data Trends Report:
May 8-November 8, 2000

Overview

The Internet Fraud Complaint Center (IFCC) is a partnership between the National White Collar Crime Center (NW3C) and the Federal Bureau of Investigation (FBI). IFCC's primary mission is to address fraud committed over the Internet. This is done by facilitating the flow of information between law enforcement agencies and the victims of fraud, information that might otherwise go unreported.

The 2000 IFCC Six-Month Data Trends Report is the first compilation of information on complaints received and referred by IFCC to law enforcement or regulatory agencies for appropriate action. The results provide an examination of key characteristics of 1) complaints, 2) perpetrators, 3) complainants, and 4) the interaction between perpetrators and complainants. Overall, the results are intended to enhance our general knowledge about the scope and prevalence of Internet fraud in the United States.

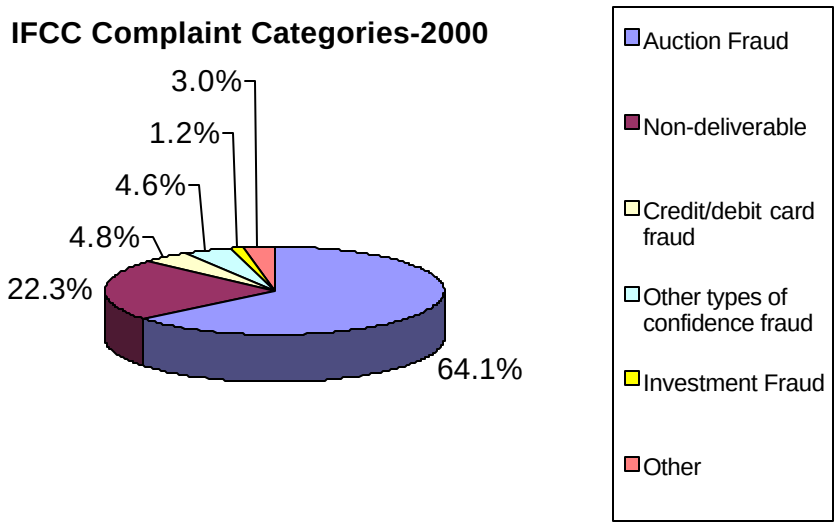
Information About the Data

The IFCC began operating on May 8, 2000. Between the inception date and November 8, 2000 the IFCC web site had received more than 37.5 million visits, and 20,014 filings were made. As of November 8, 2000, 6,087 complaints of fraud were referred to law enforcement and regulatory agencies around the world. On average, each of these complaints was referred to four agencies for further action (24,348 referrals). Of these referred complaints, 5,273 involved the perpetrator utilizing the Internet. Even though the IFCC mission is to address fraud committed over the Internet, 814 of the complaints involving only the more traditional methods of contact (e.g. telephone & in-person visits) were also referred on behalf of the individual filing a report.

Although the information in this report does give the public a unique insight into growing concerns over fraud, the results do have some limitations. The data presented here is derived from referred complaints only, and may not reflect certain groups that have not reported their victimization to any agency. IFCC analysts evaluate complaints for validity. However each referral agency makes its own investigative determination. Additionally, complaints are received exclusively through the Internet and, thus, results may be more representative of Internet users than all fraud victims in general. Despite these qualifications, the report serves as both an awareness tool for the general public and a potential information tool for groups responsible for controlling Internet-related fraud.

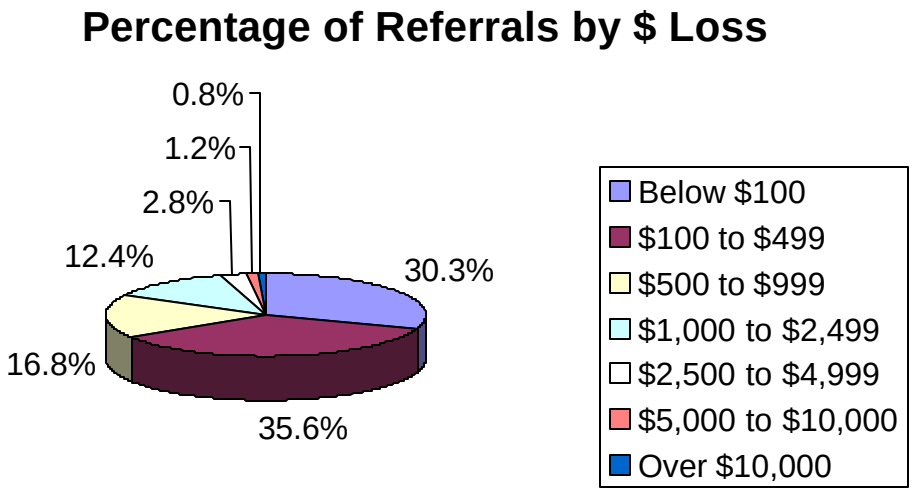
Complaint Characteristics

As has been the case since the inception of IFCC, auction fraud is by far the most reported Internet fraud, comprising nearly two-thirds of all referred complaints. Non-deliverable merchandise and payment accounts for another 22% of complaints, and credit and debit card fraud make up almost 5% of complaints. Other types of confidence fraud, such as home improvement scams and multi-level marketing, as well as investment fraud, are also among the most reported offenses. For a more detailed explanation on complaint categories used by the IFCC, please refer to the appendix at the end of this report.



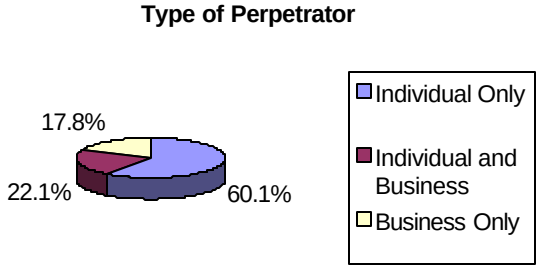
A key area of interest regarding Internet fraud is the average monetary loss incurred by complainants contacting IFCC. Such information is valuable because it provides a foundation for estimating average Internet fraud losses in the general population. To present information on average losses, two forms of average are offered, the mean and the median. The mean represents a form of averaging familiar to the general public; the total dollar amount of Internet fraud complaints referred divided by the total number of Internet fraud complaints referred. Because the mean can be sensitive to a relatively small number of extremely high or extremely low loss complaints, the median is also provided. The median is simply the 50th percentile, or midpoint, of all loss amounts for all referral complaints of Internet fraud. The median is less susceptible to extreme cases, whether high or low cost.

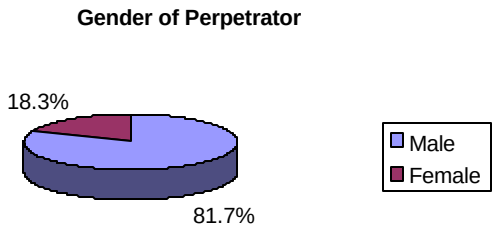
When including non-Internet fraud complaints and complaints still awaiting referral, the mean dollar loss was $1,259, with the total loss exceeding $12.3 million. The highest single dollar loss reported to IFCC during this period was $366,248. The total dollar loss from all Internet-related referred IFCC cases was $4.6 million. The mean dollar loss from Internet-related referred IFCC cases was $894 and the median was $255. Over 17% of referred complaints involved losses of $1000 or more with 83% representing cases of less than $1,000. Nearly one-third of all cases had a total loss value of less than $100, and two-thirds lost under $500. For Internet fraud, the highest dollar loss per incident is found among investment fraud victims (median loss of $500), where larger amounts of cash are usually required up-front from the complainant. The lowest dollar loss was found among auction fraud offenses (median loss of $233). Dollar loss amounts were not required on the original web-based complaint form. The IFCC now requires this information on its new complaint form, which went online January 11, 2001.



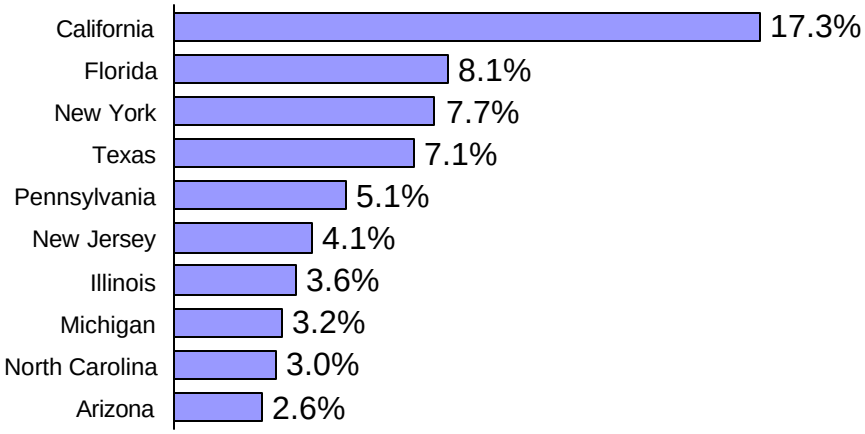
Perpetrator Characteristics

The data from the IFCC also provides insight into the demographics of fraud perpetrators. Those involved in these types of offenses tend to be individuals (as opposed to businesses), male, and residing in some of the larger states in the country. They come from a varied international background, with a significant representation in the U.S., Canada, and Eastern Europe. Although the top ten states for perpetrators very closely mirrors that of complainants, there are variations. Arizona and North Carolina have high numbers of Internet fraud offenders, the latter state having the highest rate of overall fraud arrests according to recent UCR data. This lends some support to the notion that the IFCC trends, while still new, are beginning to resemble those of other official crime statistics on fraud.

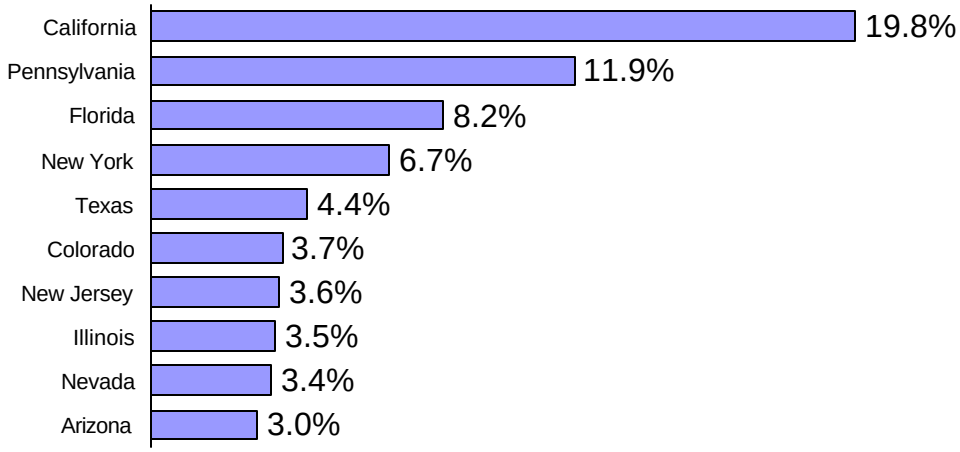




Top Ten States:Individual Perpetrator



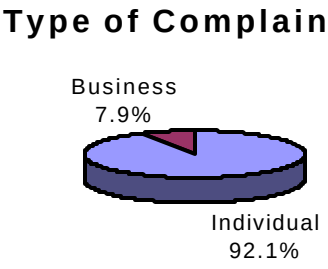
Top Ten States:Business Perpetrator

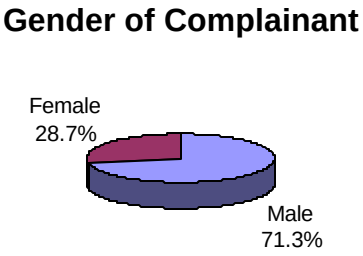


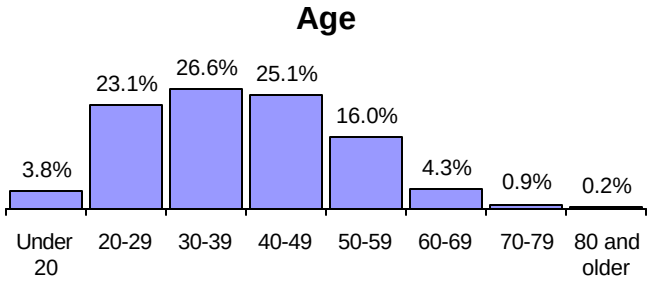
Top Ten Countries:Perpetrators

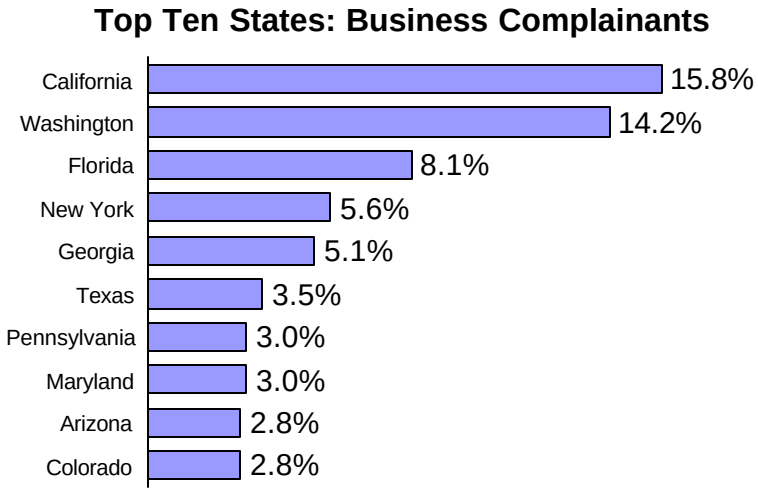
Complainant Characteristics

The following graphs offer a detailed description of the typical Internet fraud complainant who reports the offense through IFCC. Overall, complainants tend to be individuals (as opposed to businesses), male, between 30 and 50 (the average age is 38.6), and reside in one of the four most populated states: California, Texas, Florida and New York. States such as Washington and Virginia, which are not as populated but tend to have higher proportions of technology companies (and Internet users), round out the states in which most complainants reside. Though the majority of complainants are individuals, it may be misleading to draw conclusions that only 1 in 10 victims reporting Internet fraud are businesses. *IFCC is not yet fully set up to handle business complaints, and therefore this group is underrepresented in the current analysis. As the IFCC evolves to meet the needs of all victims, it is anticipated that businesses will make up a larger proportion of Internet fraud complainants.*

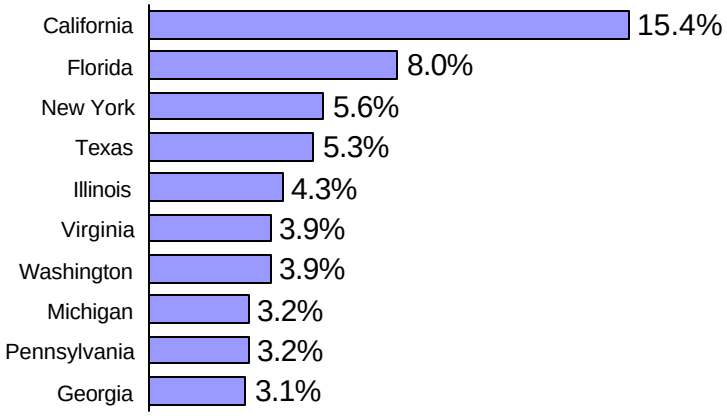








Top Ten States: Individual Complainants



Top Ten Countries:Complainants

Table 1 looks at differences between the amounts lost per incident and the various complainant demographics. Because the overwhelming majority of referrals only consist of a handful of offense types, there is little variance between victims and fraud type. However, the amount loss seems, at least in part, to be influenced by a number of factors. First, businesses lose considerably more per Internet fraud than do individuals. Males tend to lose more than females, and older individuals tend to have a higher dollar loss than younger individuals. While there isn't enough information to fully understand the differences presented here, what does stand out is that Internet fraud is costly for people from all backgrounds.

Table 1 *Complainant Demographics*	*Average (median) $ Loss per Typical Complaint*
Type	
Individual	$255
Business	$616
Gender	
Male	$330
Female	$140
Age	
Under 20	$200
20-29	$288
30-39	$255
40-49	$235
50-59	$324
60-69	$281
70-79	$285
80 and older	$610

Only one in four complainants were found to have previously sought assistance from a government agency, and that was due in part to a higher dollar-loss incident. Interestingly enough, the victim is much more likely to contact the perpetrator, although in the majority of instances the perpetrator does not offer a resolution to the problem.

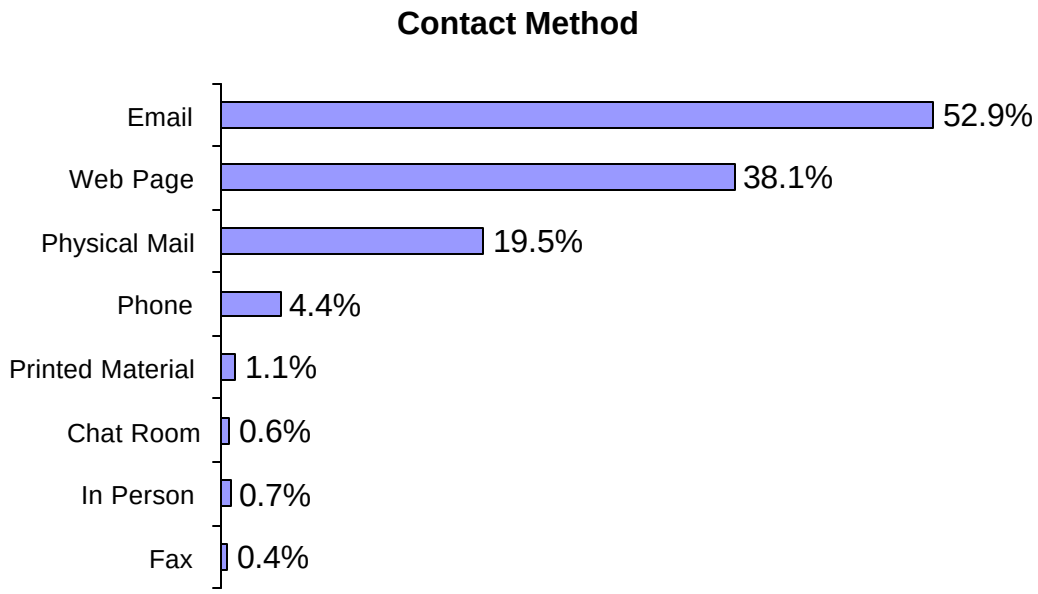
Have you contacted law enforcement or any other government agency regarding this matter?
Yes: 23.4% (average dollar loss was $425) ***No: 76.6% (average dollar loss was $210)***
Did the victim talk to the perpetrator?
Yes: 58.1% ***No: 41.9%***
Did the perpetrator offer a solution to the victim?
Yes: 9.9% ***No: 90.1%***

Complainant-Perpetrator Dynamics

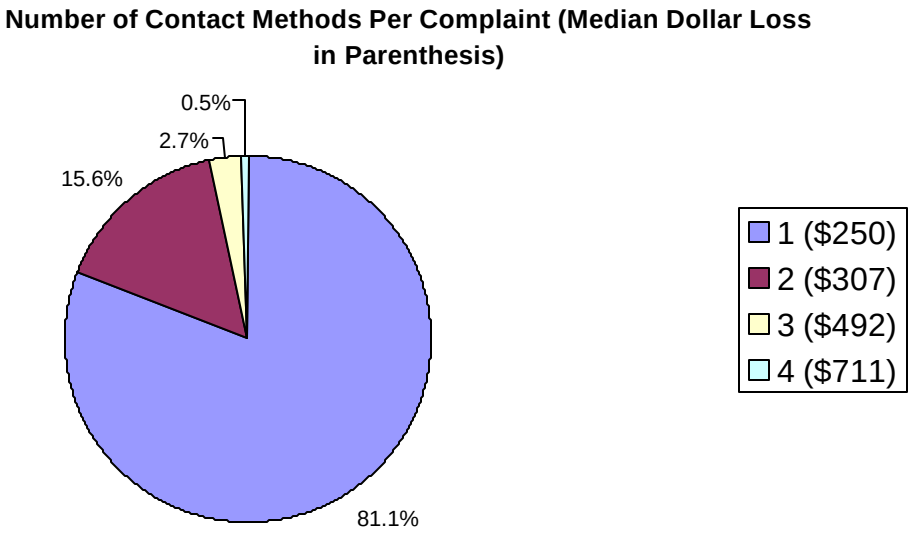
One of the components of fraud committed via the Internet that makes investigation and prosecution difficult is that the offender and victim may be located thousands of miles apart. This is a unique characteristic not found with many other types of 'traditional' crime. These jurisdictional issues often require the cooperation of multiple agencies to resolve a given case. Table 2 highlights this truly 'borderless' phenomenon. Even in California, where most fraud seems to originate, only 22% of referred cases involve both a complainant and perpetrator residing in the same state. Other states have an even smaller percentage of complainant-perpetrator similarities in residence. These patterns seem to not only indicate 'hot spots' of perpetrators (California for example) that can target potential victims from around the world, but it appears that most complaints probably involve complainants and perpetrators that did not have a relationship prior to the incident.

Table 2: Complainant's State	*% of Perpetrator's From Same State (Other top perpetrator locations in parenthesis)*
California	22.2 (8.0 from Texas, 7.7 from New York, 6.2 from Florida, 6.1 from Pennsylvania)
Florida	13.3 (18.8 from California, 9.0 from Pennsylvania, 7.1 from New York, 3.8 from Texas)
New York	11.1 (23.8 from California, 8.7 from Florida, 6.3 from Pennsylvania, 6.3 from Texas)
Texas	9.2 (18.7 from California, 8.4 from Florida, 8.0 from Pennsylvania, 4.0 from Arizona)
Washington	5.8 (17.3 from California, 12.8 from New York, 5.8 from Pennsylvania, 5.8 from Texas)
Illinois	6.3 (15.1 from California, 7.8 from New York, 7.3 from Florida, 6.3 from Texas)
Virginia	4.3 (20.9 from California, 11.0 from New York, 11.0 from Florida, 8.0 from Pennsylvania)
Michigan	5.8 (13.7 from California, 9.4 from Florida, 7.9 from New York, 7.9 from Texas)
Pennsylvania	16.0 (14.6 from California, 9.7 from Florida, 9.7 from New York, 6.3 from Texas)
Georgia	7.1 (18.1 from California, 11.0 from Florida, 7.7 from Pennsylvania, 4.5 from Delaware)

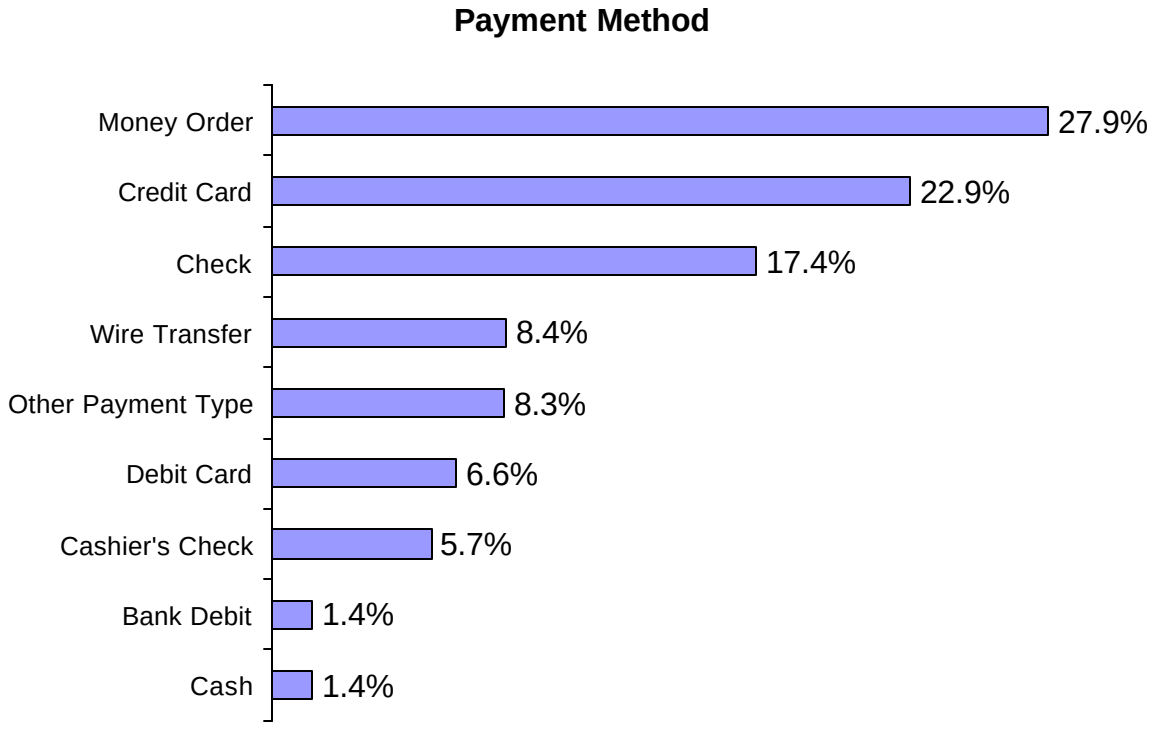
The following data provides further information on complainant-perpetrator dynamics. Email and web pages are the two primary mechanisms by which the alleged fraudulent transactions took place. Of particular interest is the high rate of email contact; the lucrative business of selling personal data, including email addresses, coupled with the explosive growth of individuals with email accounts may be contributing to this phenomenon.



Another interesting trend that has emerged is the dynamics between different contact methods. Almost one in five complainants indicated that they had two or more different contact methods with the perpetrator. For example, this may have involved an email followed up with physical mail or the complainant visiting a web page. The amount lost also increased when the number of different contact types increased. This could be due to more complex schemes, involving multiple contacts, or situations in which complainants were asked for money on more than one occasion.



The next chart describes the various payment methods used by complainants. Money orders were the most common method employed, while credit card and check payments were also common. Debit cards, cashier's checks, and cash make up a smaller portion of the payment methods.



Conclusion

The data suggests that the typical victim reporting to IFCC tends to be a male, in his mid 30's, residing in one of the more populated U.S. states, and was involved in a fraudulent online auction transaction that resulted in the loss of over $200. While this typology might depict the 'average' complainant, it is important to note that anyone is susceptible to falling prey to an Internet fraud. The IFCC has received complaints from both males and females ranging in age from ten to one hundred years old. Complainants can be found in all fifty states, in dozens of countries worldwide, and have been victimized by everything from work-at-home schemes to identity theft. As online usage continues to climb, particularly among groups who are currently underrepresented, the face of the typical victim might certainly change in the upcoming years.

With the widespread adoption of technology in the everyday activities of consumers come new opportunities to commit fraud and other forms of computer-related criminal activity. The move to action has been slow, due in part to the public's lack of information regarding the prevalence and threat of Internet crime. Exponential changes in technology, and the growth of online usage itself, make it difficult to accurately portray the problem. The IFCC is in the unique position to meet these needs. Through the online complaint and referral process, victims of Internet fraud are provided with an easy way to alert authorities, at many different jurisdictional levels, of a suspected criminal or civil violation. The IFCC Six Month Data Trends Report also serves the public through the identification of current fraud patterns and trends. By understanding the risks, Internet users can better protect themselves from becoming the victims of online crime.

* * *

Appendix: Types of Internet Fraud

Analysts at the IFCC determine a fraud type for each Internet fraud complaint received. IFCC analysts sort complaints into one of nine fraud categories.

- Financial Institution Fraud- Knowing misrepresentation of the truth or concealment of a material fact by a person to induce a business, organization, or other entity that manages money, credit, or capital to perform a fraudulent activity. [1] Credit/debit card fraud is an example of financial institution fraud that ranks among the most commonly reported offenses to the IFCC.

- Gaming Fraud- To risk something of value, especially money, for a chance to win a prize when there is a misrepresentation of the odds or events.[2] Sports tampering and claiming false bets are two examples of gaming fraud.

- Communications Fraud- A fraudulent act or process in which information is exchanged using different forms of media. Thefts of wireless, satellite, or landline services are examples of communications fraud.

- Utility Fraud- When an individual or company misrepresents or knowingly intends to harm by defrauding a government regulated entity that performs an essential public service, such as the supply of water or electrical services.[3]

- Insurance Fraud- A misrepresentation by the provider or the insured in the indemnity against loss. Insurance fraud includes the "padding" or inflating of actual claims, misrepresenting facts on an insurance application, submitting claims for injuries or damage that never occurred, and "staging" accidents.[4]

- Government Fraud- A knowing misrepresentation of the truth, or concealment of a material fact to induce the government to act to its own detriment.[5] Examples of government fraud include tax evasion, welfare fraud, and counterfeit currency.

- Investment Fraud- Deceptive practices involving the use of capital to create more money, either through income-producing vehicles or through more risk-oriented ventures designed to result in capital gains.[6] Ponzi/Pyramid schemes and market manipulation are two types of investment fraud.

- Business Fraud- When a corporation, or business knowingly misrepresents the truth or conceals a material fact.[7] Examples of business fraud include bankruptcy fraud and copyright infringement.

---

[1] Black's Law Dictionary, Seventh Ed., 1999.
[2] Ibid.
[3] Ibid.
[4] Fraud Examiners Manual, Third Ed., Volume 1, 1998.
[5] *Black's Law Dictionary, Seventh Ed., 1999. The Merriam Webster Dictionary, Home and Office Ed., 1995*.
[6] Barron's Dictionary of Finance and Investment Terms, Fifth Ed., 1998.
[7] Black's Law Dictionary, Seventh Ed., 1999.

- Confidence Fraud- The reliance on another's discretion and/or a breach in a relationship of trust resulting in financial loss. A knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment.[8] Auction fraud and non-delivery of payment or merchandise are both types of confidence fraud and are the most reported offenses to the IFCC.

[8] Ibid.