Fraud in the Digital Environment: Facts and Figures

Over the years, as technology has improved, so has fraud. Fraudulent acts such as credit card, identity, or tax fraud, have increased tremendously; raising concerns for internet safety. Credit card fraud is one of the most common types of internet fraud in the country. Online spending and lack of government security has allowed many predators to take advantage of unsuspecting victims. To know more about this fraud, we must know what it is, how it occurs, and ways to prevent it.

According to Cornell Law School, “credit card fraud is a form of identity theft that involves an unauthorized taking of another’s credit card information for the purpose of charging purchases to the account or removing funds from it.” (Staff, 2006) When it comes to credit card fraud, victims often do not know they are victims until after their credit card has been used. Credit card fraud can affect people in-person or on the internet. Typically, in-person fraud occurs because a card is either lost or stolen. Once a criminal has possession over the card, they can use it on whatever merchandise they want. They can also take however much money they want. Some people get their credit card information stolen online too by having malware sent to e-mail, clicking on a fake website, and even forgetting to securely make a purchase. Technological advances have created hackers that can gain access to someone’s credit card information with ease. “In the United States, card-not-present fraud is already a big problem. In fact, it accounted for 45 percent of credit card fraud in 2014, followed by counterfeit card fraud (37 percent) and lost/stolen cards (14 percent).” (Holmes, 2015)



“The total value of card-not-present transitions is expected to grow from $9 billion in 2013 to nearly $19 billion in 2018.” (Holmes, 2015) More people are doing their shopping online, rather than going to stores to shop. In doing that you, will have to know which websites are safe to use so that someone does not gain access to your card information. Credit card fraud can also occur when a person prints an illegal credit card using a fake name. Credit card fraud is so common that it is not as easy to tell if you are getting scammed, or not with the advancement of the criminals today. But, there are some signs that can help someone identify if they are being defrauded. For instance, getting your credit card bill with numerous purchases that you have not made, finding that your card has been declined for insufficient funds, and getting packages at your door that has your name on them, but you do not remember ordering them.

To prevent credit card fraud, the consumer must be careful when searching or browsing websites. Websites that obtain sensitive information will tend to have certain characteristics on the screen that consumers can see. This allows for the person to know that site is secure to their information. A prime example of this would be a simple lock character. It is located either on the search bar of that website, or at the bottom of the page. Many do not know what this lock means, or they do not pay enough attention to the screen. It is critical to look for this sign. Another basic aspect that one should know, would be signs of other people using this website for purchases and having positive feedback. Seeing that other people have used a website and having good feedback is a positive sign that a site is secure for credit cards. If there is any way of identifying that a site is safe in this way, it should not be used if there may be scammers or black-market deals going on. Another safety aspect of credit cards is the EMV chip. The EMV chip is an “embedded microprocessor that store[s] and protect[s] cardholder data.” (FAQ, n.d.) The chip is said to be the next step in preventing fraud and increasing card security. As stated by Chase, EMV chip technology requires the consumer to provide a PIN and a signature. Although a signature may not be required after every transaction, providing the PIN number by itself is just as safe.

 Finally, credit card fraud is one of the most dangerous and common fraudulent acts of the twenty-first century. Innocent browsing and routine use of the internet have victimized billions of internet users. To remain protected, not only against credit card fraud, but all fraud, is to be aware of red flags while using the internet. Browse websites with caution and use credible websites. Protect personal information with strong passwords and security questions. Many may find themselves in the middle of a credit card scheme, and by the time they catch it, thousands of dollars have been spent falsely under their name.

If you are looking for additional information, here are a list of sites below:

“Credit Card Fraud (2017)

<https://www.nw3c.org/docs/research/credit-card-fraud-2017.pdf>

“Credit card fraud and ID theft statistics”

<http://www.nasdaq.com/article/credit-card-fraud-and-id-theft-statistics-cm520388>

“Fraud”

<https://legaldictionary.net/fraud/>

References

Holmes, Tamara. “Credit card fraud and ID theft statistics.” *NASDAQ.com*, 16 Sept. 2015, [www.nasdaq.com/article/credit-card-fraud-and-id-theft-statistics-cm520388](http://www.nasdaq.com/article/credit-card-fraud-and-id-theft-statistics-cm520388).

Staff, L. (2007, August 06). Credit Card Fraud. Retrieved February 25, 2018, from <https://www.law.cornell.edu/wex/credit_card_fraud>

Chegg.com. (n.d.). Retrieved February 25, 2018, from <http://www.chegg.com/homework-help/identity-theft-identity-fraud-occurs-someone-else-s-personal-chapter-2.1-problem-10ayu-solution-9780321838704-exc>

FAQ: Chip-Enabled Card Acceptance (EMV). (n.d.). Retrieved February 25, 2018, from <https://www.chasepaymentech.com/faq_emv_chip_card_technology.html>