Free research paper about the impact of identity theft on consumer and businesses...

Business, Company

Anita Evensen

The occurrence of identity theft has not seemed to diminish with today's technological advances. On the contrary, it seems to be more prevalent than ever before. " In 2012, for instance, about 12. 6 million Americans were reportedly victims of identity fraud. This is an increase from the approximately 11. 6 million who were victimized in 2011 and 10. 2 million who were victimized in 2010."

Previously, it was harder for anyone to steal personal information. Short of actually stealing your wallet and credit card, thieves would either have to watch someone enter a credit card number or go dumpster diving for financial records, such as checks, credit card statements, and pay stubs. Nowadays, anyone's information can be hijacked electronically, whether it happens during an online purchase or a purchase at a cash register. Unfortunately, even the best internet security software cannot protect consumers adequately from credit card fraud. The FBI makes the following recommendation for consumers for using a credit card online: " Don't trust a site just because it claims to be secure."

Identity theft is not a joke to the people who suffer from it. Whether someone was able to get a hold of health information or a credit card number, it's easy to see the type of damage that can result from it. The least harmful incident of identity theft is when someone has merely stolen an individual's credit card information. Generally, such a thief will " request new account PINs or additional cards, make purchases, [or] obtain cash advances."

In most cases, victims can dispute the charges with the bank or credit card

company and get the card replaced without financial consequences to themselves.

However, when someone gets a hold of a person’s social security number and other financial data, it can be hard to clean up the mess afterwards. If the victim’s credit score is good enough, the thief could apply for a loan in the victim’s name without his or her knowledge. It can take months to find out that this has even happened. The victims of identity theft will either see it on their credit report or find themselves talking to a debt collector with a company they’ve never heard of before.

The most frustrating aspect is that it is really difficult to catch the criminals. After all, they haven’t used any of their personal information. If they applied for a loan at a bank in person, it might be possible for law enforcement to search through tape recordings of the video camera the bank has. However, it will be very difficult to identify them that way. In most cases, the criminals don’t get caught, which is one of the reasons they attempt to steal information in the first place.

In order to keep personal and financial information safe, individuals need to be cautious about giving it out. For example, it could be a bad idea to enter your social security number online. Before applying for a loan, credit card, or a line of credit, individuals need to verify that the website they’re using is safe and not part of a scam. Individuals need to be especially cautious about email solicitations inviting them to click on links. Individuals should also understand that a social security number is not needed for everything. For example, a new patient form at a doctor’s office may ask for it, but that doesn’t mean it needs to be filled out. In most instances, a driver’s license

number is enough for identification purposes.

Organizations are under even more pressure than individuals to keep the data they collect safe. With recent credit card fraud affecting big chain stores, such as Target and Michael’s, every company has become aware of the responsibility they carry. This might mean adding extra security measures to their credit card processing system.

However, even small companies are affected by identity theft. Every company has to store a lot of sensitive information about their employees. This means they are required to keep their employee records locked away safely. Not only does this require locks and keys, but the employer also has to ensure that HR and accounting employees are trustworthy enough to have access to the information they need.

The three companies that may have the largest hassle with identity theft are the three credit bureaus Equifax, Experian, and TransUnion. In order to purchase a copy of a credit report, each of these credit bureaus has to check carefully who is requesting the information. And when identity theft is discovered, these credit reporting agencies have to spend a lot of time setting things right. Consumers who are wary of identity theft may also decide to freeze their credit. This in turn creates even more work for the credit bureaus, but it stops potential thieves from applying for a loan in someone else’s name.

Identity theft is a real concern for both individuals and companies. When someone goes shopping with a stolen credit card, either the store or the credit card company has to eat up those charges. The merchandise is gone, but nobody has paid for it. These costs will get passed down to each and

every consumer indirectly. That’s why it’s really important for every individual to monitor credit card spending, bank accounts, and activity on his or her credit report. “ If you report fraud within two days of receiving your statement, your liability is limited to $50.” Most credit card companies are already spending a lot of time and money on monitoring the accounts for potential fraud. Consumers will need to follow their lead and keep an eye on their credit report as well.

References

Finklea, K. (2014). Identity Theft: Trends and Issues. Congressional Research Service.

Howard, C. (2013, January 1). Credit Freeze and Thaw Guide. Retrieved July 3, 2014, from ClarkHoward. com: http://www. clarkhoward. com/news/clark-howard/personal-finance-credit/credit-freeze-and-thaw-guide/nFbL/

U. S. Department of Justice. (n. d.). Internet Fraud. Retrieved July 03, 2014, from The Federal Bureau of Investigations: http://www. fbi. gov/scams-safety/fraud/internet_fraud

Vaas, L. (2013, March 06). How to protect yourself from debit-card fraud. Retrieved July 03, 2014, from Naked Security: http://nakedsecurity. sophos. com/2013/03/06/how-to-protect-yourself-from-debit-card-fraud/

Webroot Inc. (2014). Credit Card Fraud. Retrieved July 03, 2014, from Webroot: http://www. webroot. com/us/en/home/resources/articles/pc-security/malware-credit-card-fraud