solutions to identity theft

Posted on September 21, 2018

Identity theft is a criminal activity where criminals impersonate the identity of another person and commit crimes (Reyns, 2013). Identity theft includes activities where one can access passwords, credit card numbers, and social security card numbers. When such crucial information falls into the hands of criminals, they use it to commit crimes where owners end up in debt or lose money from their banks. Identity theft has become rampant as criminals are finding advanced techniques for infiltrating information systems without the knowledge of organizations (Federal Trade Commission, n.d.).

Bachenheimer, S. I. (2013). *U.S. Patent No. 8,396,747*. Washington, DC: U.S. Patent and Trademark Office.

Bachenheimer provided a solution to identity theft mainly for users who engage in online purchases and transactions. Controlled cards use a platform where users can subscribe to their identities and personalized data to be encrypted to improve security. The system, according to the author, will improve the security of cardholders by hiding personal details whenever they use it for online transactions. The partnership with such agencies will provide continuous protection to cardholders from the access of personal information on e-commerce sites. If customer data is breached, institutions offering such services will be held responsible, allowing users to recover their funds.

The findings and proposals of the research provide additional mechanisms for dealing with identity theft. In enhancing research on this topic, it will be important to look into the various ways of dealing with identity theft. This article will provide much-needed information for analyzing the role that third parties can play.

Bose, I., & Leung, A. C. M. (2013). The impact of adoption of identity theft countermeasures on firm value. *Decision Support Systems*, *55*(3), 753-763.

Identity theft has negative impacts on firms, particularly engaging in e-commerce. The adoption of e-commerce has been declining because of numerous cases of identity theft (Bose & Leung, 2013). In the article, the authors review the impact of embracing measures that counter the risk of identity theft. The authors unanimously agree that a firm’s value will improve if it provides security measures to counter identity theft. The adoption of such countermeasures improves and establishes the trust and confidence of users in the company's information systems. The move will generate traffic, which will see the adoption of e-commerce and online payments on the rise.

Analyzing the value of a firm when it adopts better measures of dealing with identity theft helps in promoting a safe online environment. The suggestions from the article will help explain the benefits of putting up countermeasures against identity theft. The article provides relevant information from experienced authors who add credibility to the article.

Chambers, V., & Zeidan, R. (2013). *Stopping Tax Identity Theft: Practical Advice for CPAs and Clients. Journal of Accountancy*, *215*(2), 60-64.

The study provided practical advice to the public on various ways of stopping identity tax theft. As noted by Chambers and Zedan, Identity thieves had found a new method of getting away with tax obligations and seeking refunds from the tax authorities. Through various identities, the thieves file tax returns before the official period to prevent matching information and stop the tax authority from sending duplicate return notices. The authors cautioned CPA professionals to advise their clients to protect their social security cards and always be at the forefront in helping clients file their returns. The research further urged clients to monitor their tax accounts continually and report any suspicious links to the tax authority.

The information provided in this source highlights the extent of identity theft, even in tax institutions. Research is crucial in expanding knowledge on this topic and formulating policies to combat identity theft.

Gerstner, L. (2016). Guide to Protecting Yourself from 5 Types of Identity Theft. *Kiplinger's Personal Finance*.

In the article, the author brings to the public the increasing cases of identity theft that have seen large companies lose millions in the process. Data breaches are a means by which hackers are used to access social security numbers and other personal details of citizens to be used for fraud. Government information systems, as well as those of financial institutions, have been hacked several times, and clients' data has been breached. In the article, the author provides two mechanisms that can be used by organizations to prevent data breaches. The author highlights the need to observe cautiously at all times. The author additionally urged organizations to put up strong measures to combat cyber-attacks.

The information from the article has diversified the various ways in which thieves can access private information. The measures proposed are important in the study as they provide advanced techniques for dealing with data breaches.

Gerstner, L. (2016). Seven Smart Moves to Prevent Identity Theft. *Kiplinger's Personal Finance*, *67*(9), 58.

In the article, Gerstner notes identity theft is on the rise as hackers are coming up with better technologies for accessing personalized information. Gerstner assesses the danger of identity theft and provides seven techniques that can be employed to protect one from identity theft. Safeguarding security numbers and avoiding falling into online fraud is highlighted by the author. Gerstner proposes that information that could be used by hackers and secure systems with strong passwords be destroyed. Protecting the account, taking a credit freeze, and securing gadgets are the other moves that the author feels can protect one from identity theft. These moves, when applied, will go a long way to reduce cases of identity theft.

The information provided in the article helps to expand knowledge on various ways of combating identity theft. The article is recent and authored by an expert, which is good when used for scholarly research.

He, B. Z., Chen, C. M., Su, Y. P., & Sun, H. M. (2014). A defence scheme against identity theft attack based on multiple social networks. *Expert Systems with Applications*, *41*(5), 2345-2352.

Social media is a platform that has advanced identity theft. Users often disclose their personalized information, such as names and locations, which can easily be accessed by fraudsters. The same information can be used to generate new profiles with the same details and used for criminal activities. The authors note that social media has promoted identity theft, which has seen friends break up. The research entails proper defense schemes that can be used to deal with the rising cases of identity. The authors propose verification of social media identities to allow the user to identify with the real owners. Verification will help stop the use of fake identities to engage in criminal activities.

The research has diversified identity theft to include the use of social media. The findings of the research call for immediate action to be taken to address the rising cases of identity theft in social media. It will be crucial to develop policies to address identity theft in social media.

Hille, P., Walsh, G., & Cleveland, M. (2015). Consumer fear of online identity theft (Hille et al., 2015): Scale development and validation. *Journal of Interactive Marketing*, *30*, 1-19.

Consumers continue to display fear when it comes to online identity theft. Online platforms and online routines continue to pose a danger to consumers and other users. In the article, the authors provide a solution to the problem through the process of scaling development and validation. The scale of development uses different scales portrayed by consumers when it comes to their proneness of identity theft. Once the scale has been established, a validation program is developed to approve the usage of online platforms. The findings still open doors for further research but set the basis for dealing with the fear of using online platforms.

The findings and analysis of this source widen the scope of identity theft beyond fear. Fear of online theft can be quantified, and appropriate measures can be put in place to improve user confidence. The research opens doors to further research in the same field. It is recent and credible based on the backgrounds of its authors.

Holtfreter, K., Reisig, M. D., Pratt, T. C., & Holtfreter, R. E. (2015). Risky remote purchasing and identity theft victimization among older Internet users. *Psychology, Crime & Law*, *21*(7), 681-698.

Identity theft takes various forms and is mostly perpetrated through the internet. In the article, the authors point out that older people are the majority victims of identity theft. Older people are mostly targeted because of their low self-control and their high susceptibility to online fraud. They are most likely to open links in their emails and make remote purchases without authenticating the source of the email. As older people are duped through solicited emails, they fall prey to hackers who can then access their personal information and engage in high-degree crimes. Older people are, therefore, urged to exercise caution on online platforms.

The research targets old people who have limited knowledge of cybersecurity. Their low self-control puts them in danger of identity theft. Fraudsters target this group of people with the aim of getting their information. The research will be crucial in analyzing various groups in society that are likely to be targeted and affected by identity theft.

Interview

The interview involved a sales manager at an Auto Expo location in New York City who provided information on the topic of identity theft. According to the manager, identity theft was part of the problem that was affecting its online businesses. Identity theft has led to numerous cases of clients losing funds. Their data was additionally used to engage in crime, which increased the debt obligations of the clients. Identity theft had furthermore increased lawsuits where clients had been arrested for criminal offenses. Identity theft had worked against the company, which had seen a slight reduction in its sales. The company had moved to improve the security of its online platforms with the aim of enhancing customer confidence.

The interview is important in improving the research as it provides primary information on companies affected by identity theft. It will help in developing appropriate measures to counter the problem of identity theft.

Kahn, C. M., & Liñares-Zegarra, J. M. (2016). Identity theft and consumer payment choice: Does security really matter? *Journal of Financial Services Research*, *50*(1), 121-159.

The article addresses the issue of security when it comes to online payments. The two authors talk about the rising cases of fraud that have seen a reduction in the acceptance of credit cards and other online payment solutions. Identity theft has affected the means of doing business, and businesses are looking into alternative payment methods to prevent possible lawsuits involving data breaches. In the end, the authors come to a common understanding of the importance of security in online transactions. Security enhances trust and promotes the growth of the business. The absence of secure networks will deter both the users and owners from the use of credit cards.

Security is important when it comes to payment options. Secure networks prevent identity theft, which promotes the use and acceptance of credit cards. The findings will be of benefit in analyzing security issues related to identity theft. The article is also recent, which adds credibility when used in research.

Saleh, Z. (2013). The Impact of Identity Theft on Perceived Security and Trusting E-

Commerce. *Journal of Internet Banking and Commerce*, *18*(2), 1-11.

The impact of identity theft is far-reaching, and this was the basis of the research conducted by Saleh. The objective of this study was to determine consumers' perceptions of e-commerce businesses because of increased cases of identity safety. The research found that customers had developed a negative perception towards e-commerce due to the numerous cases of identity theft. Most consumers noted the increased cases of online theft that had led to massive losses as the main cause of mistrust in these platforms. Customers are now considering other means of purchasing goods since e-commerce puts their personal information at risk. The author concluded the research by urging e-commerce businesses to put up techniques for securing customer data.

The research advances the area of identity theft by assessing the impact of increased cases of theft in e-commerce. The findings will enrich my research on the impact of identity theft.

Seda, L. (2014). Identity Theft and University Students: Do They Know, Do They Care? *Journal of Financial Crime*, *21*(4), 461-483.

In this article, the author sought to investigate university students' knowledge of identity theft and the various preventive methods that could be used to combat the rising cases of identity theft. Seda found out that university students were knowledgeable about the existence of identity theft but took no initiative to understand measures for reducing identity theft. Students cared less about identity theft as they were less affected. The author summarized the research by urging universities to come up with strategies for creating awareness on the issue of identity theft among students. The target audience for the research was university students and university administration.

The research is perfectly suited to address the missing links in identity theft among university students. The author's contributions and findings will help enrich the research by providing the perspective of identity theft among students. The article is recent, which makes it resourceful evidence.

Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine

activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency*, *50*(2), 216-238.

Reyns research sought to find out the relationship between online routines and the risk of identity theft. Findings indicated individuals who engage in numerous online activities are at risk of identity theft. The author particularly noted that individuals who engage in Internet banking are more exposed to identity theft due to unsecured systems. Online shopping, particularly e-commerce, exposes individuals to a higher risk of theft. Downloading behaviors, as well as messaging activities such as the use of email, put the information of the users at risk. Males and high-income persons were identified to be at higher risk for identity theft because they are highly victimized. The findings put much blame on online routines as the major cause of online theft.

The research provides a unique perspective on studying online behaviors and the risks they pose to individuals. The information from this source will be helpful in the research, as it will provide a unique perspective on online behaviors.

Roberts, L. D., Indermaur, D., & Spiranovic, C. (2013). Fear of cyber-identity theft and related fraudulent activity. *Psychiatry, Psychology and Law*, *20*(3), 315-328.

The article points out that identity theft is on the rise, mainly on online platforms. Identity theft has increased fear among users, particularly in the use of the internet. The authors point out that one in twenty-five people in Western countries are affected by fraudulent activities because of identity theft. The statistics are alarming since such figures increase fear of using online platforms. The authors point out such cases to curtail the progress of e-commerce since individuals are worried about the security of their cards. The impact of identity theft has psychological effects on those affected. The author calls for the improvement of cybersecurity to protect users and prevent rising cases of psychological problems.

The research will be crucial in addressing the psychological problems associated with identity theft. The findings of these authors will form the basis of enriching the study. It is additionally recent, and the background of the authors adds to the credibility of the source.

Villa-Real, A. E. C. (2014). *U.S. Patent No. 8,831,677*. Washington, DC: U.S. Patent and Trademark Office.

The author provides a solution to identity theft, particularly on online platforms. In the proposal, the author suggests the use of customer-controlled instant response technologies that allow them to notify relevant authorities of potential identity theft. The gadgets, according to the author, will provide a mechanism for users to report cases of identity theft immediately to authorities so that credit cards can be blocked from access. The author blames poor communication as the main cause of rising cases of identity theft. Individuals usually find it hard to report incidents to authorities for immediate action. The communication barrier has led to these cases, and a solution to the communication barrier can help to avert the problem.

The research provides a real solution to this problem. It will be extensively explored to enrich the study. The suggestion presented in the article will be analyzed with the aim of developing better mechanisms for dealing with identity theft.

References

Bose, I., & Leung, A. C. M. (2013). The impact of adoption of identity theft countermeasures on firm value. *Decision Support Systems, 55*(3), 753–763.

Federal Trade Commission. (n.d.). *What to know about identity theft*.

Hille, P., Walsh, G., & Cleveland, M. (2015). Consumer fear of online identity theft: Scale development and validation. *Journal of Interactive Marketing, 30*, 1–19.

Holtfreter, K., Reisig, M. D., Pratt, T. C., & Holtfreter, R. E. (2015). Risky remote purchasing and identity theft victimization among older Internet users. *Psychology, Crime & Law, 21*(7), 681–698.

Kahn, C. M., & Liñares-Zegarra, J. M. (2016). Identity theft and consumer payment choice: Does security really matter? *Journal of Financial Services Research, 50*(1), 121–159.

Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency, 50*(2), 216–238.

Roberts, L. D., Indermaur, D., & Spiranovic, C. (2013). Fear of cyber-identity theft and related fraudulent activity. *Psychiatry, Psychology and Law, 20*(3), 315–328.