Credit Monitoring Application: Protect Children from Child Identity Theft

Chua Zi Liang[1], Intan Farahana Kamsin[2], Zety Marlia Zainal Abidin[3] and Hemalata Vasudavan[4]
[1'2'3'4]Asia Pacific University of Technology and Innovation, Technology Park Malaysia, Bukit Jalil, Kuala Lumpur, Malaysia
[1]tp061556@mail.apu.edu.my, [2]intan.farahana@staffemail.apu.edu.my, [3]zety@staffemail.apu.edu.my, [4]hemalata@staffemail.apu.edu.my

***Abstract* - Data breaching is a security infringement widely used by the hackers to gain certain information or data with unauthorized access which threaten countless organizations and individuals. It has been an unpreventable cyber threat since 2005 by grabbing the attention of the public to start concerning data breaching but limited solutions are provided to prevent this cyber-attack. Furthermore, one of the most crucial types of data breaching is child identity breach. At this point, there was still no solution to stop child identity theft, parents and guardians are only able to minimize the risk of their child's identity breach. In this proposal, a reliable Children's Data Breaching solution is being proposed to protect the children by enhancing the Credit Monitoring Applications to better protect the children's identity under 18.**

***Index Terms* - Child Identity Fraud, Data Breach, Cyber Crime, Cyber Security, Credit Monitoring Application**

1. Introduction

As technologies are getting advance and the cybercrimes are continue increasing, data breach has reached the point of no return. Data breach happens when one or more parties are permitted to retrieve the data to which they are not authorized. The occurrence of data breaching has created a conducive environment for all types of identity theft. Identity theft was not just a major topic until recently, however it was a widespread issue even before the internet and technology era. Traditionally, identity thieves were being called as "dumpster living" [1], they will walk around a targeted area searching in garbage bins to look for personal information namely abandoned invoices and data that identified an individual.

In 2018, there were 14.4 million of identity theft cases being reported [2] and 1 million victims out of the 14.4 million victims are children [2]. A child's identity can be utilized for the same purposes as an adult's identity, such as financial benefit and healthcare. If the attacker is a family member or close contact of the family, this can consider as a type of familiar identity theft [3]. The main reason of child identity theft is that underage youngsters typically do not comprehend or aware of the significance of personal information. When the children have become an adult who is mature enough to utilize his/her information for office purposes, they realized they've became the victims of this crime.

A strong cyber security application like credit monitoring application is being utilized to reduce the risk of identity theft but most of the applications are only focusing on monitoring a specific type of identity theft. Hence, this research paper will concentrate on enhancing a credit monitoring services by fixing the issues stated in the problem statement and to provide a solution by developing a stronger credit monitoring application.

2. Literature Review

2.1 Research Domain

2.1.1 Child Identity Theft

The digital era has introduced a new variety of threats for parents to safeguard their children, from cyberbullying to sexting to kidnappers, and that range of threats has now grown to include child identity theft. The online experience has changed the childhood of most of the children in the 21st century. It allows children to explore the world, but it also allows the world to explore a child's information and life if there's no proper precautions taken.

Child identity theft is crime where a thief steals a child's identity and uses his/her personal information to create bank accounts or make mobile purchases [4]. Such crime might go unnoticed for years because children do not file taxes or apply for loans [4].

According to the research from Marchini & Pascual, there are more than 1 million of children were the victims of identity theft in the year of 2017. This resulting a total loss of $2.6 billion and more than $540 million were paid by the families out of their pocket.

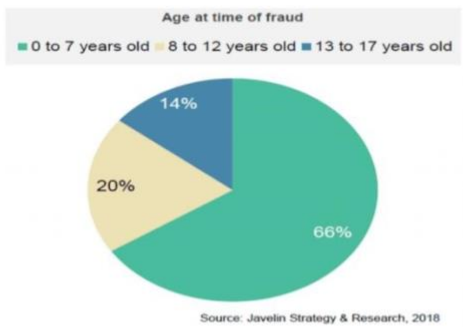

Figure 1: Age at Time of Fraud

Based on the figure 1, the pie chart has shown twothirds of the identity fraud victims were children aged 7 and under in the year of 2018 [5]. One of the main reasons why children aged 7 under are more likely to be one of the victims in 2018 is because the identity theft could be a familiar identity theft. Children aged 7 and under are still not able to fill in some difficult personal information such as IC number, passport number, date of birth and full home address.

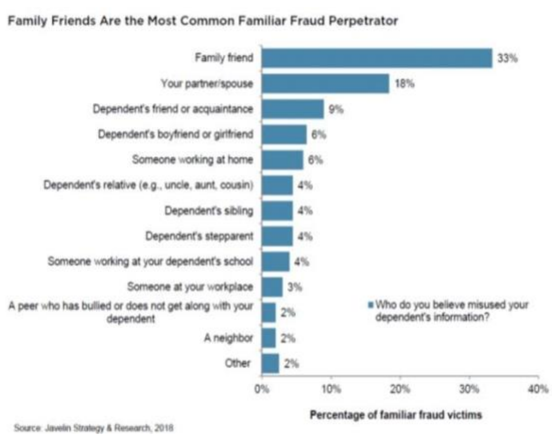

Figure 2: Family Friend Are the Most Common Familiar Fraud Perpetrator

Based on figure 2, family friends are the most common familiar identity theft [5]. Therefore, figure 2 can be a strong and supportive research for proving that most of the identity theft for children aged under 7 are familiar identity theft in 2018.

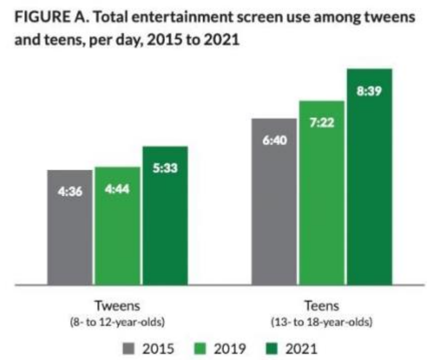

Figure 3: Total Entertainment Screen Use Among Tweens and Teens per day (2015 to 2021)

On the other hand, research from Ofcom has shown that nearly all children aged 3-17 in 2021 have their own social media profiles. Figure 3 has shown that the total amount of screen time used by the children has an obvious increment especially from 2019 to 2021 [6]. The main reason of this can be the epidemic, Covid-19 where everyone is only allowed to socialize and study via online [7].

In conclusion, child identity theft is a very serious problem if parents and guardians do not know how to protect their children from cyber threats. Based on the study above, child identity theft is transforming into a more crucial issue for children because the identity theft is everywhere which they can't prevent. Therefore, a solution must be provided to protect the children.

2.1.2 Credit Monitoring

Credit monitoring is a service or application that tracks and monitor changes of an individual's credit report, for example it monitors credit scores and look for any fraudulent activities. Besides, it also allows an individual to monitor his/her credit health, identify vulnerabilities and detect indicators of identity theft.

The credit file provides details regarding an individual's credit history. User may view the credit accounts created, the amount of debt owed, whether making on-time payments, and Personally Identifiable Information (PII). Credit report monitoring may assist user in keeping track of everything and alerting them to activities such as credit scores, any related information added to user's credit file and new public records.

Normally, credit monitoring provides 3 bureau credit monitoring that notifies users the changes of their credit reports. The 3 credit bureaus are TransUnion, Equifax and Experian. Without the protection of these 3 bureaus, user might overlook inaccuracies in their credit reports [8].

2.1.3 Credit Monitoring Application to prevent Child Identity Theft

Child identity theft is more common while many people realize. It's logical to believe that adolescents with no credit records aren't a victim for this crime. According to Equifax, minors are frequently exploited as "blank slates" to apply for loan or acquire loans since they lack credit histories, and their credit is frequently left unchecked [9]. It is prohibited for anybody under the age of 16 to apply for a loan, but relatively few organizations use official documents to check ages [10].

According to the study from Javelin, nearly 90% of the family with internet connection declare that their children are accessing social media [10]. Most of the children aged 3-18 has their own gadgets or tablets and are using their own profile to access social media such as Twitter, TikTok, Facebook, Instagram and Twitch. Predators and cybercriminals remain hidden of all social media sites, waiting for the perfect opportunity to prey on excessively trusting youngsters who may not completely comprehend safe online behavior. Children without supervised online have unpredictable high risk to get their identity exposed.

While the threat from identity theft might be frightening for parents and children, there are solution parents can take to safeguard their child's identity online. Credit monitoring application can be consider adopted for children to protect them from child identity theft and parents can monitor and be aware of the social media or websites their children are accessing. Parents can consider a credit monitoring application with security freeze function to freeze their child's credit report [11].

2.2 Similar System

2.2.1 IdentityForce

Figure 4: https://www.identityforce.com/

Figure 5: https://www.identityforce.com/

IdentityForce is an application providing credit monitoring and identity theft protection services which has a reliable reputation, having a 4.5 TrustScore on TrustPilot and approximately 800 client ratings [12]. IdentityForce provides daily monitoring of credit reports for their clients from the three main credit bureaus which is Equifax, Experian, and TransUnion, along with SMS and email notifications whenever a charge or account withdrawal exceeds a monetary level their clients choose. Besides, it provides social media monitoring that monitors client's social media, namely Twitter, Facebook, Instagram and YouTube accounts for improper or abnormal activities. IdentityForce also includes online anti-phishing and anti-keylogging software to keep their clients safe when shopping online.

2.2.2 Credit Sesame

Figure 6: https://www.creditsesame.com/

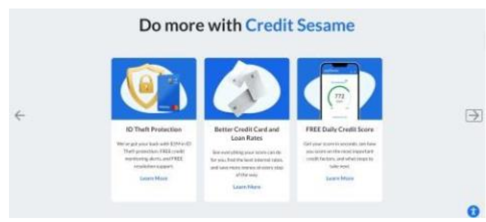

Figure 7: https://www.creditsesame.com/

Credit Sesame, similar IdentityForce, is an application that provides credit monitoring and identity theft prevention services. Sesame Credit has been active for over 10 years, and it shows debt data as well as assists users in understanding credit scores. It provides some free function such as basic credit and tracking tools, but to activate the Focused Credit view, users must subscribe to the premium tier. It has many benefits such as free subscription tier, a wonderful user experience, tracking and analysing debt, and reporting on rent payments, but it also has downsides which include the premium tier being costly and the free tier lacking capabilities that many competitors provide[13].

2.2.3 Comparing Similar System

System / Features / Components	IdentityForce	Credit Sesame
Fraud Insurance	Covered	Covered
Dark Web Scanning	Yes	No
Credit Bureaus Monitoring	3 Bureau : Equifax, Experian and TransUnion	1 Bureau : TransUnion
Charges	Intermediate to Expensive	Free
Social Security Monitoring	Yes	No
Credit reports monitoring	Daily	Daily
Mobile Application/Version	Smartphone and Tablets	Smartphone and Tablets
Children monitoring	Yes	No

Similar

Table 1 : Similar system comparison table

The table(*Table 1*) above displays the features and components of the systems that are similar to the proposed system of this research. The features or components that would be heedful of are Fraud Insurance, Dark Web Scanning, Credit Bureaus Monitoring, Social Security Monitoring and Children Monitoring. This system has to be both Mobile and Web Application to scan through all kinds of vulnerabilities on mobile and web. It has to be free for download in the Play Store, App Store and Websites, whereas being approved and governed by the government.

3. Problem Statement

Children's identity was being targeted by the criminals retrospectively to late 1990s and has since evolved into the organized crime it is today. It has become an uncontrollable cybercrime that sends a shiver of fear through parents and grandparents. However, parents typically don't monitor their children's identities since a child's identity is a blank slate, and the probability of discovery is low, as the child will not be using it for a long period of time.

A child's information is being stolen and used by the so-called "synthetic identity theft" [12] to create a synthetic identity which is a combination of real and fictitious information. The ID stolen were used to purchase homes and automobiles, open credit card accounts, secure employment and obtain driver's licenses [14]. Use of a child's Social Security number for fraudulent purposes may not be detected for years [14]. The potential impact on a child's future is profound as it could destroy or damage a child's ability to get the approval on student loans, obtain a job, acquire a mobile phone or secure a place to live. Children can present a blank slate for fraudsters because they generally don't have credit reports [12].

Based on the problems mentioned, there are still no complete solution for child identity theft. Therefore, a solution needs to be developed to protect and prevent the child identity breach from the child identity theft.

4. Research Aims

The aim of this research is to develop a reliable Children's Data Breaching solution to protect the children by enhancing the Credit Monitoring Applications to better protect the children's identity under 18 years old.

5. Research Objectives

i. To provide identity theft insurance for all the children with a reasonable cost.

ii. To implement Security freezes function to prevent access to children's credit reports.

iii. To implement a powerful monitoring system of all three credit bureaus (Credit Bureau Malaysia Sdn Bhd; CTOS Data Systems Sdn Bhd; and. Experian Information Services (Malaysia) Sdn Bhd.

7. Methodology

7.1 Sampling Method

To conduct this research smoothly and effectively, stratified sampling is being utilized to find out why cases of child identity breach keep on increasing. The quantitative research will include a simple survey that ask questions about the awareness of parents toward child identity breach and the mobile or website applications children are accessing. The survey will be conducted via online platform to reach out to people in other states. In this research, survey is selected to conduct the survey because a huge and consistent number of data need to be collected to achieve better understanding of the selected targeted group. Interview will not be a good choice for the research since an amount of data is needed to obtain from a large group in a limited time given. Thus, quantitative research with survey method will be the best choice to conduct this research.

7.2 Identify Respondents

The targeted respondents for this survey are parents with kids and children under 18 with social media profile primarily. Reason for this is that these respondents are the main people that are currently finding for a solution to prevent them from child identity theft, and they can impact the people around them. Besides, cybersecurity experts are also included as the respondent of this survey since child identity theft is currently a solemn problem facing by most of the people. Therefore, everyone must stand up against this cyber threat to protect our next generation.

7.3 Sample Size

This survey will be conducted with 150 respondents ranging from the subgroups, parents with kids, children under 18 with social media profile and cybersecurity experts. The responds will not be limited to only 1 state in Malaysia, instead it will cover up all states of Malaysia. This can also provide a more accurate data for this research which all the respondents in every state will have different opinions.

8. Overview of the Proposed System

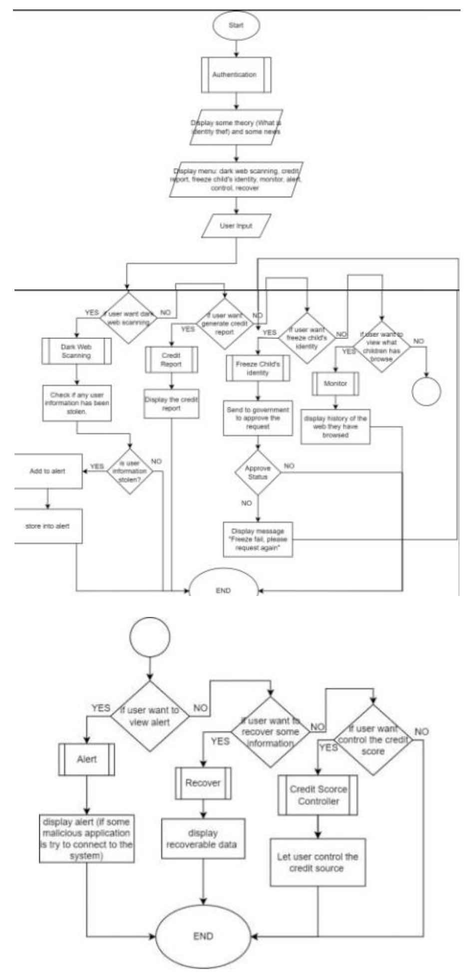

Figure 8: Overview of the proposed system

Figure 10 shows the proposed system's flow chart and the system operating flow. There a login system to authenticate the user identification when the proposed system is launched. If the user successfully signs in, it will display a series of information to the user, such as what identity theft is, how it impacts our life, and recent news regarding identity theft. The system will provide some function for the user to click on if they wish to use the feature. The functions that may be performed include dark web scanning, credit report generation, freezing child's identity, monitoring, alerting, controlling, and recovering.

The main goal of this proposed system is to freeze the child's credit report to prevent third parties from deceiving or stealing it, resulting in the child losing their credit score and having a major impact, such as being unable to obtain a student loan or secure a living place after the child grows up. To summarize, this proposed system not only performs the functions listed above, but it also provides the theory of identity theft and the most recent news to raise the parent's or user's awareness of identity theft and child identity theft.

9. Conclusion

Criminals targeted children's identity theft in the late 1990s, and it has now evolved into organized crime. It is a serious issue that disturbed parents, and it could not be ignored today, because the consequences of this problem will severely harm children's futures. As a result, the aim and objective of this research were detailed in this paper, as well as the strategy for implementing and improving the solution and the overview of the proposed system. The research will then be carried out using a stratified survey to identify the reason of the growth in child identity theft. Moreover, the questionnaires will be selected to obtain massive data on the target population through online platforms, and will be able to obtain the opinions of people in various states of Malaysia to ensure the accuracy of the data. Furthermore, the proposed system, "credit monitoring application" came into being by comparing with similar systems IdentityForce and Credit Sesame, which would prevent access to child identities and block any malicious application. The proposed system may freeze a child's credit record and isolate identity theft to safeguard children while also raising parental awareness of child identity theft. With this system, incidences of child identity theft may be effectively decrease, and the child credit report could be kept clean to safeguard our nation's future pillars.

References

[1] Shareen Irshad, Tariq (2018, Feb). Identity Theft and Social Media. 43-52. Retrieved May 4, 2022, from https://www.researchgate.net/profile/Tariq-Soomro-2/publication/323185128_Identity_Theft_and_Social_Media/links/5a850d2aa6fdcc201b9f044c/Identity-Theft-and-Social-Media.pdf

[2] Al Pascual, Kyle Marchini (2018, April 24). *2018 Child Identity Fraud Study*. Retrieved from Javelin: https://www.javelinstrategy.com/research/2018-child-identity-fraud-study

[3] Betz-Hamilton, A. (2020, August). Understanding the Experiences of Familiar Identity Theft Victims. *Journal of Financial Therapy*, 90,103-104. Retrieved May 3, 2022, from https://newprairiepress.org/cgi/viewcontent.cgi?article=1237&context=jft

[4] Masterson, K. (2022, March 16). *Criminals Target Children for Identity Theft and Fraud*. Retrieved April 2, 2022, from AARP: https://www.aarp.org/money/scamsfraud/info-2022/child-identity-theft.html

[5] *Child Identity Fraud Costs Nearly $1 Billion Annually, According to a New Study From Javelin Strategy & Research*. (2021, Nov 2). Retrieved May 6, 2022, from BusinessWire: https://www.businesswire.com/news/home/20211102005484/en/Child-Identity-Fraud-Costs-Nearly-1-Billion-AnnuallyAccording-to-a-New-Study-From-Javelin-Strategy-Research

[6] Victoria Rideout, A. P. (2021). Media Use by Tweens and Teens. *The Common Sense Census*, 12-45. Retrieved from https://www.commonsensemedia.org/sites/default/files/research/report/8-18-censusintegrated-report-final-web_0.pdf

[7] Moyer, M. W. (2022, March 24). *Kids as Young as 8 Are Using Social Media More Than Ever, Study Finds*. Retrieved May 3, 2022, from nytimes: https://www.nytimes.com/2022/03/24/well/family/child-social-media-use.html

[8] White, A. (2022, April 28). *The best credit monitoring services that can help you spot fraud early*. Retrieved April 29, 2022, from CNBC: https://www.cnbc.com/select/bestcredit-monitoring-services/

[9] EquiFax. (2022). *How Can I Better Protect Against Identity Theft?* Retrieved May 4, 2022, from Equifax: https://www.equifax.com/personal/education/identity-theft/how-to-protect-againstidentity-theft/

[10] DiNardi, G. (2022, May 16). *How To Protect Your Child From Identity Theft*. Retrieved May 5, 2022, from Aura: https://www.aura.com/learn/how-to-protectyour-child-from-identity-theft

[11] Texas. (2022). *How to Protect Your Child or Teen from Identity Theft: Cybersecurity Best Practices*. Retrieved May 4, 2022, from Texas: https://techbootcamps.utexas.edu/blog/howto-protect-your-child-or-teen-from-identitytheft-cybersecurity-best-practices/

[12] Grant, K. B. (2018, April 24). *Identity theft isn't just an adult problem. Kids are victims, too*. Retrieved April 2, 2020, from CNBC: https://www.cnbc.com/2018/04/24/childidentity-theft-is-a-growing-and-expensiveproblem.html

[13] TRETINA, K. (2022, March 7). *Best Credit Monitoring Services*. Retrieved April 29, 2022, from Investopedia: https://www.investopedia.com/best-creditmonitoring-services-4846982

[14] Power, R. (2011, Mar 29). *Child Identity Theft*. Retrieved from Cylab: https://eriskhub.com/files/articles/article229.pdf

[15] Chansen, R. L. (2018). What is Synthetic Identity Fraud? *The Evolution of Synthetic Identity Theft and Its Impact on Children*, 1-6. doi:13421600

[16] Dyke, J. V. (2022, Feb 3). *DATA BREACHES: FUEL FOR THE IDENTITY THEFT AND FRAUD FIRE*. Retrieved May 2, 2022, from SONTIQ: DATA BREACHES: FUEL FOR THE IDENTITY THEFT AND FRAUD FIRE

[17] Equifax. (2022). *Are My Children at Risk Of Identity Theft?* Retrieved May 1, 2022, from Equifax: https://www.equifax.com/personal/education/identity-theft/child-identity-theft/

[18] EquiFax. (2022). *How Can I Better Protect Against Identity Theft?* Retrieved May 4, 2022, from Equifax: https://www.equifax.com/personal/education/identity-theft/how-to-protect-againstidentity-theft/

[19] Kitten, T. (2021, Nov 2). *child identity Fraud: A Web of Deception and Loss*. Retrieved May 4, 2022, from Javelin: https://www.javelinstrategy.com/research/child-identity-fraud-web-deception-and-loss

[20] McNally, G. R. (2005). Identity Theft Literature Review. Retrieved May 13, 2022, from Identity Theft Literature Review