ForwardEdge AI

Business Model Analysis Applied to the Cellular Fraud Ecosystem

Quentin Adolphe

August 10, 2022

Business Model Analysis Applied to the Cellular Fraud Ecosystem

Written by

Quentin Adolphe
Forward Edge AI
Email: quentin@forwardedge-ai.com

Edited and reviewed by
Amos Townsend
Federal Management Systems, Inc.

Karthika Vadivel
Forward Edge AI

Kathy Stokes
AARP

Dr. Lethia Jackson
Bowie State University

Abstract: Scammers around the world target individuals of all demographics with low-cost technology that enable huge sums of money to be stolen in short periods of time. Losses to fraud in the U.S. total billions every year, but despite numerous efforts from governments and other organizations there seems to be no signs of the problem slowing down. This paper dives into the methodologies used by scammers through the application of a business model analysis to understand how these criminal enterprises operate. Scam businesses are so profitable because costs are kept to a minimum and individuals within the fraud ecosystem are able to focus on their discrete tasks, allowing them to become extremely efficient. Unfortunately, the solution to scams may not be the constant improvement of technology to prevent them, rather, it may be providing better economic opportunities for the fraudsters to assimilate into their community and allocating government resources more efficiently to fight this problem.

1. Introduction

Adaptability is rooted in humanity; without it, we would inevitably be consumed by our environment. All around the world fraud criminals have stolen billions of dollars from millions of victims of all demographics despite numerous defense measures being taken by individuals and organizations. Forward Edge AI is at the forefront of Artificial Intelligence (AI) and blockchain technology and is using its resources to develop intricate defenses against scam calls and texts. With the development of the Gabriel app, Forward Edge AI has created an inexpensive yet effective means of preventing fraud. Other companies have created and implemented their own scam-blocking applications giving victims a wide variety of options to choose from. Organizations like the AARP dedicate time and resources to educating the elderly and their families about the dangers of fraud, and numerous federal agencies also devote resources to consumer education. Further, the Federal Trade Commission (FTC) reports to Congress about how citizens are being impacted by scams. Despite all these efforts, however, criminals continuously adapt their practices often, making it difficult or impossible to permanently stop scams. Taking a different approach to fraud may be necessary for stopping this global issue.

Business models are commonly used by companies to outline how to make profits. Though the methods may differ slightly in their implementation, generally all have the same key structure. Tracking the flow of money is key to creating an accurate depiction of company growth. Understanding what resources are needed, how they will be allocated, and eventually how consumers will interact with the business will allow a company to efficiently grow with their markets.

Untangling the complexities of scam centers can allow companies, law enforcement agencies, and other organizations to discover new means to combat fraud. Making certain aspects of the scam business model more expensive or challenging to execute can lead to less profitability and therefore decreased motivation to continue the operation.

2. Business Model

2.1 Value proposition

Scam centers provide “value” in many different forms. Only focusing on one aspect would not be sufficient. While there may be more or less effective ways to provide value, it differs for every victim and caller. Kathy Stokes, director of fraud prevention programs with AARP, describes how a scammer might go about providing a false sense of value in their sale, “whether it’s fear … ‘your grandson is in trouble’, … [or] ‘your Social Security number has been used in a crime and there's a lot of trouble here I think we can help you’... or it’s ‘you won a car and a million dollars’” (K. Stokes, personal communication, June 30, 2022). In journalist Snigdha Poonam’s article on scammers in India, she noted that “[t]he way to scam Indians at such a scale, apparently, is to promise them jobs – the fulfillment of their most cherished dream” (Poonam, 2018). These scenarios clearly differ greatly in terms of their content but what they all share is their ability to put a victim into a heightened emotional state. To be effective, a scammer must understand who they are talking to, skillfully crafting their story to manipulate their victim. A scammer will then carefully begin to take from their victim by creating false value, or a solution to whatever problem the victim faces. These solutions can take many forms, but the general concept remains evident – we can solve your problem with a large payment or by sharing your sensitive information.

2.2 Customer segments

Scammers will target anyone with money. A common misconception is that older people are targeted more. On the contrary, younger people report experiencing and losing money to scams far more often than older people. However, when older people are targeted, they are typically impacted to a greater extent. It is important to note that this data may not accurately represent the severity of fraud in each demographic, as the FTC only has access to reported data and is subject to the willingness of victims to communicate their situation. Younger adults typically do not have much money to lose. Stokes explains young adults can "lose 200 bucks from a tech support scam, [and] though it may be hard [they] will survive it. But they don't have more than 200 bucks [to lose]" (K. Stokes, personal communication, June 30, 2022). 2022 Federal Trade Commission data verifies these findings, with all adults under the age of 60 reporting median losses of less than $600. This contrasts significantly with many elderly people who have saved money their entire lives. Given similar circumstances, you may see an instance where "a young person loses $200, [but] you might see an older person, say in their 80s, lose $50,000 because [they] have it to lose. But [they're] also in a place in [their] life where [they] can't make up for that, and that money is almost always just gone." Similarly, the FTC finds that victims between the age of 70 and 80 years old report median losses of $1000, and median losses of $1,800 for those who are 80 years or older as seen in Figure 1 (Federal Trade Commission, 2019). It is important to note that FTC data encompasses reports only; many victims don't report so incidents and losses are likely far higher. Significant financial loss makes scams and fraud very difficult for the elderly to recover from. Their vulnerability stems from the devastating outcome they experience after the damage has already been done. While young people may in general be more vulnerable to scams, elderly victims often do not have the capacity to deal with large-scale monetary loss as they no longer have a stable source of income or the ability to rejoin the workforce to recoup their losses.

Mark Solomon, International Association of Financial Crimes Investigators (IAFCI) international first president, believes that nearly anyone with money is a target but young adults and seniors are especially susceptible. Seniors are usually "the most financially secure, [they] put money aside… and they're available to scams because many of them are retired." (M. Solomon, personal communication, July 8, 2022). Targeting seniors is one way scammers increase efficiency in their operations. Having money readily available means victims will have little to no buffer against quick money exchanges. Rapid interactions with scammers decreases the amount of time a victim can think, forcing the loss of rationality that is so critical in dealing with any emotionally elevated situation. The vulnerability in younger adults may arise from their lack of familiarity with scams. Unsuspecting young adults often may not know what to look for, leaving them vulnerable to attacks.

2.3 Key activities

Most activities necessary to run SMS or phone scams take place online. Mark Solomon states "unfortunately a lot of the bad guys have access to the same tools that law enforcement and banks do, like search software…where you can look up peoples [Personally Identifiable Information]". Once personal information is obtained, it can be bought, sold, or traded all online. Additionally, with such large amounts of data available on the internet, scammers can tailor their purchases to their exact needs with relative ease.

This vast availability of information importantly reduces the technological

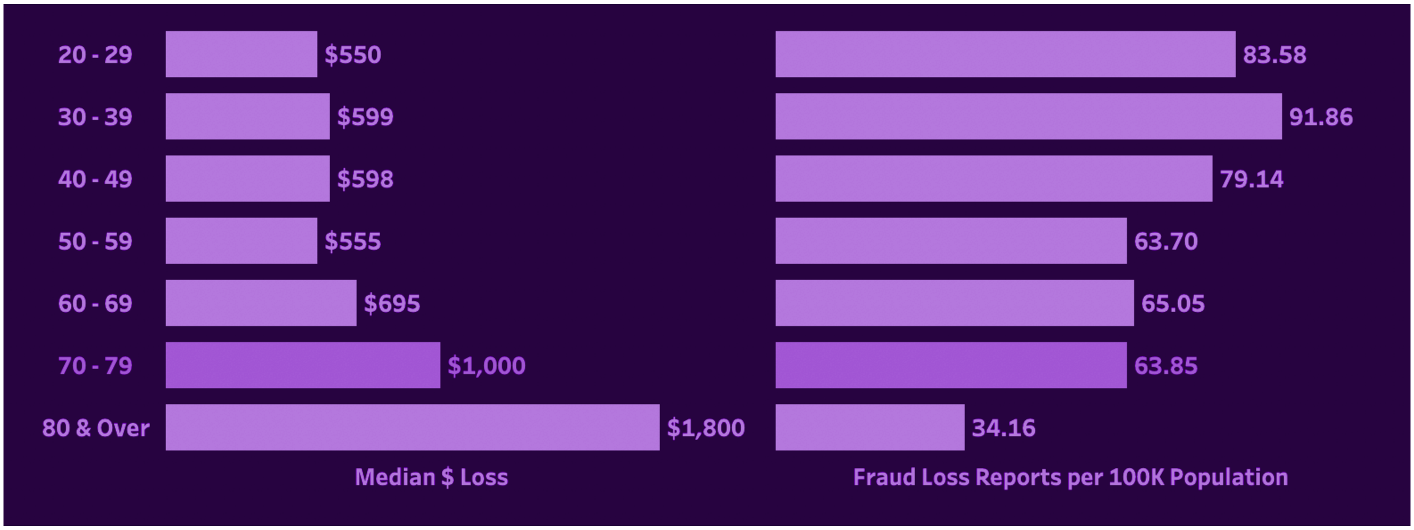

Figure 1: Median losses to scams and number of reported losses per 100K population by age. From Federal Trade Commission (2019)

knowledge required to successfully run a scam. Contrary to popular belief, the illegal purchasing of private information does not need to take place on the dark web. Messaging services like Telegram are often used to conduct business. Hurdles that may have been present a decade ago have been substantially reduced with the development of smarter technologies. A scammer can choose many routes to conduct their business, whether that means fulfilling duties themselves or outsourcing work to others online. It is vital to acknowledge that criminals will use any technology available to them to conduct business. In many ways, committing fraud is easier than ever, and improving technology and cyber security may not be the most effective way of stopping fraud.

2.4 Key Resources and Costs

Scam operations in the US are mostly small, consisting of individuals who buy cheap phones, laptops, identity-hiding software, and information-finding software like LexisNexis. Notably, cases like when inmate Jesse Lopez along with his cellmate were able to conduct a fully functional scam operation from behind bars are becoming common. The only piece of technology they used from prison was a smuggled cell phone along with apps to hide their identity (Shadel, 2021). Scam operations are increasingly popular because of the extremely low startup cost. SMS or phone scams are cheap ways for anyone to make huge profits.

Larger and more sophisticated operations can incur higher expenses. Certain scams like Medicare fraud may require illegitimate involvement from legitimate medical professionals, labs, and access to durable medical equipment, for example, but often these elements serve no practical purpose to the public (Dunkel, 2014). Overseas scam operations can also look different, taking the structure of a more traditional business. Solomon describes how a center might function with “boiler rooms set up…for a month, hiring 20, 30, 40 people to do around-the-clock phone calls.” Running larger operations like these generate much higher operating costs, but also greater returns. There cannot be one generalized cost structure to encompass all SMS and phone scam operations. However, the use of commonly available technologies such as phones, laptops, and applications seem to be consistent throughout the fraud ecosystem.

Furthermore, large scale operations, specifically those not residing in the U.S., generally have ‘required training sessions.’ Snigdha Poonam recounts her time as a journalist applying to a scam center job in India, secretly collecting information and testimonials to uncover information about these illegal operations. At the job interview Poonam was briefly questioned about her background and English-speaking proficiency but mostly remained in the dark about any details regarding the company. The interviewer reluctantly offered her the position but was abrasive and resisted revealing any information about the company. Poonam then had to pay the interviewer 500 rupees for her time.

Upon arrival at training, Poonam paid an additional 1000 rupees to attend the class. The seminar lacked substance, however, Poonam noted two major details from the instructor. They were that spoken English and emotional manipulation are “key to a call-center job” (Poonam, 2018).

Poonam’s experience highlights that these centers will minimize expenses wherever possible. These operations will not give out free training meaning the business takes on significantly less risk in hiring new employees. Before even beginning to defraud victims, the operation has already made money off its employees.

Additionally, Poonam’s testimony reveals an operation’s need for mentally strong and oftentimes emotionally numb individuals. These fraudulent businesses bluntly outline how to be successful in the trade. The requirement of speaking good English displays the company's targets, overseas victims usually residing in the United States. The better a scammer speaks English, the more successful they will be. These trainees have to be ruthless in their victimization, openly manipulating everyone they contact and commonly justifying their actions by believing their victims are inferior individuals. Finding individuals to fill these criteria would be expensive and time-consuming for traditional businesses, but through their brash recruiting tactics, scam operations can quickly recruit employees with minimal costs.

2.5 Key Partnerships

As with many criminal operations, partnerships are often informal and off the records. Fraud criminals will conduct business online with individuals willing to buy or sell goods. This includes people buying and selling personal information as well as people who teach other tactics on scams. Knowledge is most likely passed down within organizations/groups as well.

The fraud ecosystem is largely defined by cooperation. Solomon highlights there are such a large number of potential victims that competition is not the largest concern in an operation. An individual operation will usually find their own niche in the market, specializing their scam to whatever fits their needs, or more likely, conducting scams based on how they were taught by other criminals. Knowledge is often handed down to younger workers in addition to the discussion of tactics and strategies online. Similar to traditional businesses, scammers need to understand their landscape and adapt to ever-changing circumstances. However, unlike conventional companies with very limited customer segments, the fraud ecosystem has an extensive pool of targets to scam, thus negligible need for any competition between stakeholders. Individuals within the ecosystem are extremely willing to partake in mutually beneficial trades of information and tactics amongst each other.

Stokes notes the symbiotic relationship that exists on the internet between criminals stating, “a lot of the processes along the way in the fraud business, they’re discrete processes.” Individuals who specialize in collecting personal data will spend their time stealing that information. That information is sold to others, like call centers, who will use it to commit fraud. Depending on the operation, more specialized roles can be produced. For example, certain scammers may need to have someone legitimize stolen gift cards allowing them to be used in stores. While operations may compete for caller time, there may be unknown overlapping with each other in business partnerships. Purchasing customer data from the same source or laundering money through the same vendors are two likely scenarios in which this overlap may occur. Similarly to developing a cost structure, it is difficult to generalize business practices between all SMS and phone scam operations. Each operation buys and sells information according to its own needs which differ based on tactics, geographical location, and individual expertise.

2.6 Customer Relationships

2.6.1 Manipulation tactics

The interactions with victims are undoubtedly one of the most critical aspects of the scam process. Criminals skillfully utilize social engineering to establish credibility and exploit their targets. Stokes emphasizes that criminals focus on putting victims into a heightened emotional state commonly called the "ether" where critical thinking is significantly reduced. Fear or reward tactics are extremely useful in achieving this desired effect. Threatening some form of punishment like jail time or a large fine quickly puts victims into a seemingly hopeless state. Under so much pressure victims will gravitate toward any solutions they can find.

Contrastingly, a scammer may also present a reward tactic. Whether telling their victim they have won a large amount of money or even pretending to fall in love on a dating site, these criminals can exploit their victim's euphoric state just as easily (Stokes). Once critical thinking is reduced, it becomes relatively easy for a scammer to establish a false trust with their victim. A report by the Stanford Center of Longevity, Finra Investor Education Foundation, and The BBB Institute for Marketplace Trust, supports these findings, highlighting that, of those who engaged with a scammer, the majority believed the caller to "seem official" (DeLiema et al., 2019) Furthermore, of the respondents who lost money, the majority believed they were put under time pressure and that the scammer was "nice." Scammers employ as many tactics as possible to steal from their victims. Being put under time pressure further decreases rational thinking and adds a sense of urgency that significantly helps the criminals, and the friendly demeanor helps build trust with a victim. A scammer will often appear to be lending a helping hand in solving whatever problem they came up with.

2.6.2 Recurring Attacks

Recurring attacks are not uncommon in the scam industry. Like any business, scam operations want their customers to spend as much as possible. Scammers will note the type of responses each caller gives them and use that information to efficiently delegate their time towards more rewarding victims. Picking up phone calls, answering SMS messages, and engaging with a scammer will not only put you at immediate risk of a scam but also increase the likelihood you will be contacted again.

Criminals will also exploit individuals throughout the course of a single scam. Kathy Stokes cites an example where criminals become so adept at social engineering, they can create a scenario where their target will fall in love with them on dating sites or other social media platforms. Scammers can then slowly begin to leech off their victims incrementally taking larger and larger amounts of money. These tactics are extremely successful because the victim truly believes the relationship is real and often never finds out they are being deceived.

Criminals are able to repeatedly exploit these victims for extremely high returns.

2.7 Revenue Streams and Channels

Due to the illegitimacy of the business, there most likely exists no other major revenue streams other than scamming victims and selling information online. However, revenue streams will differ by operation, with some making more money selling goods online and others by directly scamming victims.

FTC data shows phone scams remain the most frequent method of fraud for older citizens in the US. With a median loss of $1,500, scam centers can quickly make immense returns on older victims. Importantly, this $1,500 figure does not include the many other methods victims can be contacted and defrauded (Federal Trade Commission, 2020). Contrastingly, among younger victims, social media and websites are by far the most frequent means of contact (Federal Trade Commission, 2019).

The means of transaction differ based on tactics used by the scammer and the age of the victim. FTC reports from 2018 and 2022 show a clear trend from 2017 to 2022, for older citizens credit cards are becoming a less frequently used means of transaction between victims and scammers in favor of gift cards. Additionally, however, wire transfers are the culprit of the largest amount of money lost by older people in 2018 despite being less frequently used in recent years (Federal Trade Commission, 2019).

The story is different for younger and middle-aged people. The 2022 report highlights that for middle-aged victims, credit cards are the most frequently used means of transaction followed closely by debit cards and payment apps like CashApp and Venmo. Young adults reported a mix of transaction mediums including high use of payment apps, credit cards, and cryptocurrency. Differences in payment methods between age groups are possibly caused by differences in technological literacy but attempting to make any firm conclusion with the available data could be inaccurate.

Furthermore, call center revenue is converted to profits at high rates because of minimized labor costs. Poonam's research reveals that on one account from India, scammers are paid "15,000 rupees a month, [and] 'whatever [they] made in dollars in one call, [they] would be paid twice the amount in rupees," this results in callers keeping 1/30 of what they steal, and the rest going to the business and managers.

3. Solutions

3.1 Protecting the Customer Segments

Victims around the world are clearly the core source of revenue for scammers, protecting these victims may be the key to stopping fraud. Poonam interviewed a former scammer, Sona Kapoor, who worked in an intranational scam center located in Delhi targeting Indians who were looking for a job. Kapoor affirmed that offering career resources was most effective in India as jobs are extremely hard to find. Victims pay for resume help or job opportunities that eventually lead them to a dead end. Importantly, Kapoor stated, "If clients called back threatening to file a police complaint, the company refunded the fee, but we got only four such calls every day" (Poonam 2018). Many victims are extremely scared to ask for help and believe there is no hope of getting their money back, which unfortunately is often true. Kathy Stokes states there is a stigma behind reporting scams. Those who often need help may be afraid to ask because of the social repercussions of revealing their vulnerability. Reporting any sort of scam or fraud an individual experiences is crucial to preventing scams. Furthermore, while stolen money is often lost forever, threatening to file police reports against a scammer can be an effective way to retrieve losses. Combining these two tactics can create a powerful method of preventing individual losses.

Difficulties arise when considering the scalability of this, however. In the U.S., reporting international fraud at the moment is not a valid option because federal agencies simply do not pursue these criminals. Moreover, successful implementation would require educating everyone susceptible to scams, which amounts to nearly every person. This would also introduce the challenge of eliminating the stigma behind reporting fraud. Breaking down these social barriers would require immense time and money, not to mention the willingness of individuals to learn about such scams. While there may be immense improvement with the education of the masses, the scale in which such a policy would be implemented makes this tactic less than ideal.

3.2 Attacking Key Resources

In recent years the internet has seen a rise in individuals attacking scammers. This phenomenon has grown largely in part due to YouTube where channels can upload their tactics for stopping scam attacks. Notably, individuals like a software engineer going by the alias Jim Browning hacks into scammers' computers. Through the use of virtual machines, a virtualization of physical computers that we use every day, Browning was able to gain access to a scam center's network in New Delhi. From there he set about contacting victims, financial institutions, and others all in an effort to prevent successful scams coming from that location. Eventually, Browning flooded their network with fake calls, crippling the operation for several hours. While effective, Browning's tactics are limited by his fear of being put in danger.

He considered using a virus to destroy the scammers' computers, but this would not only be illegal, it would also put him and his family in danger. Additionally, there was nothing on their computers vital to the operation (Shadel et al., 2021). While it would be expensive and time-consuming to restart, the operation would inevitably come back. Attacking the resources that scammers have access to is not as effective as it may initially seem. The host of legal problems that stem from hacking into centers as well as the immense knowledge required to do so severely limits the scalability of this tactic. The low cost of scam centers ensures that they will undoubtedly rise again, therefore, attacking an operation's resources should probably not be considered a viable solution to this fraud issue.

3.3 Blocking Revenue Streams

The only reason scam ecosystems exist is to generate money. Therefore, cutting off the revenue streams may be the most effective means of eliminating fraud. Perhaps a limited solution would involve monitoring and restricting the number of gift cards an individual can buy. For example, customers who intend to spend more than $1000 on gift cards can be flagged for possible risk of fraud, and subsequently helped by a cashier or assistant. In a 2021 Consumer Protection Data Spotlight report, the FTC found that the median loss to scams for Target gift cards was $2,500 per individual. These losses may be significantly limited with help from a third party. Moreover, victims who purchased Google Play store cards reported median losses of $500 (Fletcher, 2021). Realistically, there are very few reasons that anyone should purchase Google Play store gift cards totaling more than $500, with the vast majority of Android applications being less than $5 (Celi, 2022). Whether it is a warning on a self-checkout screen or a cashier providing assistance, having an extra layer of protection when purchasing expensive gift cards may help familiarize victims with the dangers of scams.

Furthermore, the evidence is clear that with the introduction of a third party, victims are far less likely to lose money after engaging with a scammer. The 2019 Stanford Center of Longevity study writes of those who engaged in a scam, only “20 percent reported that an organization, company or agency intervened or tried to intervene and stop the scam.” However, “51 percent of people who reported a third-party intervention were able to avoid losing money” (Stanford). Training bank employees or cashiers may be one of the most effective means of stopping fraud. Educating cashiers and bank tellers during job training on signs of fraud can lead to an increase in third-party interventions and eventually drive down the number of successful transactions between victims and scammers. For example, training cashiers to emphasize that gift cards are always for gifts and never for payments may help decrease the likelihood of a successful transaction. This tactic does not come without its challenges. Revamping the training requirements for cashiers and bank workers would require the compliance, cooperation, and investment of many private and public organizations. BankSafe, an AARP program, proves the viability of this approach by training frontline employees in financial institutions to identify the signs of coercion that are behind large thefts from scams. The program has seen promising results as employees trained by BankSafe were 16 times better at preventing fraud than untrained individuals and trained workers protected more than $1 million in fraud losses during the six-month pilot (Gunther et al.). Though BankSafe does not address all the challenges victims suffer from, wider implementation of the platform or similar programs is crucial in protecting individuals across the world

3.4 Examining a Scammer’s Motivations in India

Providing jobs may be the only long-term solution to fraud. Poonam’s research displays that fraud is so rampant, specifically in India, because there is simply no other means to make money for many individuals. Often for scammers, making calls for scam operations is no different than any other job. Indians can come out of college with a great education and be met with a lackluster job market (Vice and Poonam). Moreover, tens of millions of students competing over the jobs that are available complicates the hiring process. Job seekers often look to the government to find work, but it may take years from the time the job was announced for a candidate to actually get hired, only further frustrating the growing workforce (Pandey et al., 2022). Call centers are in a unique position for the educated community in India because they often only hire those who can speak English, a small portion of the general population. For a poor individual, it may not be a hard decision to work for a call center at the expense of their moral values. Revamping the economy and job market of India is clearly out of the realm of possibility in the vast majority of cases. If providing the fastest growing country in the world with a sustainable job market was easy it probably would have been done by now. Perhaps hopelessly, it seems a key tactic in substantially decreasing fraud in India is to solve the job crisis.

While these motivations may not be completely consistent throughout the world, money is the main driving factor for the majority of scammers. This unfortunately may suggest that a major solution to scams is again better economic opportunities for criminals.

3.5 Expanding the involvement of U.S. government agencies

Unfortunately, fraud has in many ways been ignored by law enforcement and legislative organizations. Losses from fraud and scams in 2020 across the U.S. was between $3.4 billion and $56 billion (LeaMond 2022). Not only were losses extremely large, but nobody knows the true extent of the problem. The U.S. has not invested enough resources in diagnosing the severity of fraud and trying to prevent it. As a result, individuals and the country are suffering. However, government agencies are effective at stopping fraud. In 2022, the U.S. Department of Justice announced criminal charges for dozens involved in a $1.2 billion health care fraud scheme. The convictions required nationwide coordinated actions by law enforcement to take down a telemedicine company executive, owners and executives of clinical laboratories, durable medical equipment companies, marketing organizations, and medical professionals (U.S. Department of Justice, 2022). Efforts are certainly rewarded when U.S. agencies dedicate time and resources to preventing fraud. These efforts are rarely devoted to individuals who lose money in seemingly isolated instances. Agencies do not spend enough effort in understanding the extent of scams in the U.S. and often ignore the struggles of people who lose relatively small but still significant sums of money. While isolated losses of a couple hundred dollars may seem insignificant to government agencies it is clear that this money adds up very quickly on larger scales, not to mention the devastating impacts it has on people. While it is no doubt extremely difficult to crack down on fraud, more work must be done in protecting individuals and treating these crimes more seriously rather than only focusing on large-scale fraud.

3.6 Taking action from many routes

The U.S. has had success in fighting scams, unfortunately only to a very limited extent. With our world becoming increasingly connected through cell phones and social media, individuals are more vulnerable than ever. Though the challenge of stopping scams may seem insurmountable, many underutilized solutions are already available to us. Educating the public on the dangers of fraud, cracking down on organized crime, and building better lives for youth will decrease the risk of scams for all.

4. References

Adolphe, Q., &amp; Solomon, M. (2022, July 8). Fraud Watch Discussion. Personal communication.

Adolphe, Q., &amp; Stokes, K. (2022, June 30). Discussion on Scam Call Networks. Personal communication.

Celi, L. (2022, July 13). Average price of Android apps 2022. Statista. Retrieved August 1, 2022, from https://www.statista.com/statistics/271109/average-price-android-apps/

DeLiema, M., Fletcher, E., Kieffer, C. N., Mottola, , G. R., Pessanha, R., &amp; Trumpower, M. "M. (2019, September). Exposed to Scams: What Separates Victims from Non-Victims? FINRA Investor Education Foundation. Retrieved July 22, 2022, from https://www.finrafoundation.org/sites/finrafoundation/files/exposed-to-scams-what-separates-victims-from-non-victims_0_0.pdf

Dunkel, T. (2015, June 1). Medicare fraud, scams spread across the U.S. AARP. Retrieved August 4, 2022, from https://www.aarp.org/health/medicare-insurance/info-2015/medicare-scams-spread.html

Federal Trade Commission. (2019, October 15). Age and Fraud. Tableau Public. Retrieved July 22, 2022, from https://public.tableau.com/app/profile/federal.trade.commission/viz/AgeandFraud/Infographic

Federal Trade Commission. (2020, October 18). Protecting older consumers report - federal trade commission. Federal Trade Commission. Retrieved July 22, 2022, from https://www.ftc.gov/system/files/documents/reports/protecting-older-consumers-2019-2020-report-federal-trade-commission/p144400_protecting_older_adults_report_2020.pdf

Fletcher, E. (2021, December 8). Scammers prefer gift cards, but not just any card will do. Federal Trade Commission. Retrieved August 1, 2022, from https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2021/12/scammers-prefer-gift-cards-not-just-any-card-will-do#end7

Gunther, J., &amp; Teaster, P. (n.d.). AARP banksafe: Protection against financial exploitation. AARP. Retrieved August 10, 2022, from https://www.aarp.org/ppi/banksafe/?INTCMP=RDRCT-PPI-BANKSAFE-05142020

LeaMond, N. (2022, January 18). Nancy Leamond on the need to raise response to increasing fraud. AARP. Retrieved August 10, 2022, from https://www.aarp.org/money/scams-fraud/info-2022/consumer-fraud.html

Pandey , V., Verma, A., &amp; BBC News. (2022, February 28). Inside the lives of India's angry job seekers. YouTube. Retrieved August 3, 2022, from https://www.youtube.com/watch?v=SbJjnGiKF4g&amp;t=227s

Poonam, S. (2018, January 2). The scammers gaming India's overcrowded job market. The Guardian. Retrieved July 22, 2022, from https://www.theguardian.com/news/2018/jan/02/the-scammers-gaming-indias-overcrowded-job-market

Shadel, D. (2021, February 23). These prisoners scammed millions from the comfort of their jail cells. Reader's Digest. Retrieved July 22, 2022, from https://www.rd.com/article/prisoner-jury-duty-scam/

Shadel, D., &amp; Wertheimer, N. (2021, April 1). Inside an international tech-support scam. AARP. Retrieved July 22, 2022, from https://www.aarp.org/money/scams-fraud/info-2021/international-tech-support-scam-exposed.html

U.S. Department of Justice. (2022, July 21). Justice Department charges dozens for $1.2 billion in health care fraud. The United States Department of Justice. Retrieved August 10, 2022, from https://www.justice.gov/opa/pr/justice-department-charges-dozens-12-billion-health-care-fraud