Beating Scams and Malicious Phone Spam: A Tunable Time-based Financial Filter to Establish Trust Between Unknown Parties

Adrian E. Garcia
EvoNexus, 5151 California Ave., Suite 150, Irvine, CA 92617. E-mail: adrian@myrobocash.com

Despite laws, do-not-call lists, and anti-spam applications, the volume of robocalls and unwanted calls has steadily grown over time. This is due to the economic incentives that are present within the telecommunications infrastructure and its users. As long as this economic incentive is not properly addressed, the cat and mouse game between regulators and spammers may never end. The RoboCash protocol proposes to address this economic incentive with a neutral time-based escrow utilizing refundable NanoDeposits, which are defined as an electronic, financial act of good faith that occurs automatically and virtually, to establish trust between two unknown parties. Bad actors lose their NanoDeposit, honest parties get an immediate refund.

Introduction

The rise of technology has outpaced the wisdom of generations. In particular, robocalls and malicious spam calls have dramatically grown over the past few years with 5.6 Billion calls placed in October 2019.[1] Due to the rise of cheap technology and access to a global population, policing bad actors has long been a cat and mouse game between regulators and spammers, otherwise known as "bad actors".[2] Regulators have not managed to properly protect the masses from spam phone calls. This is because the one of the most powerful human motivations, greed, drives bad actors to continue to find workarounds to any and all solutions proposed by regulators.

While the "Nigerian prince" scam,[3] also known as advance-fee fraud, has been around for centuries, the internet has allowed this social engineering tactic to reach a global population. In the early days of the internet and phones, the market size for potential victims was comparatively small. Nowadays, personal cell-phones are ubiquitous and adoption shows no sign of slowing down; the market size of potential victims is at the highest it has even been and growing. As such, the advance-fee fraud has evolved; phone scams vary from the IRS scams to computer virus removal, lottery/sweepstakes scams, resulting in an estimated loss of $9 Billion from everyday Americans in 2018.[4] In some tactics, like the lottery/sweepstakes fraud, $100M a year is stolen from elderly victims.[5] Figure 1 shows the steady rise in phone spam volume in the United States, despite the presence of laws and anti-spam mobile applications. The problem with the phone system is that there is economic incentive to abuse it. If this is not addressed properly, bad actors will continue to exploit this.

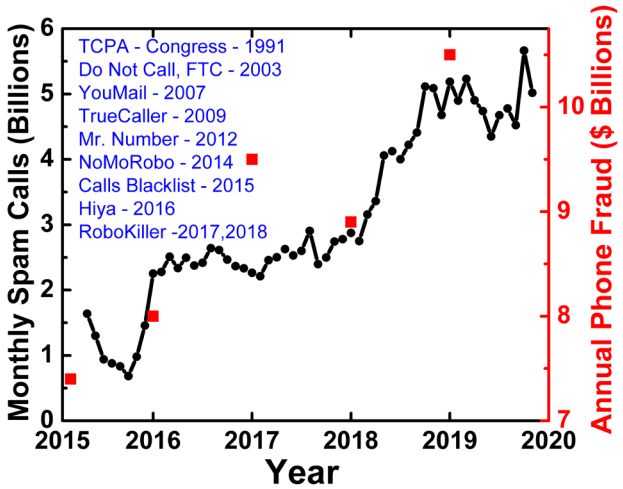

Figure 1. Black dots represent the monthly spam call volume from April 2015 to November 2019.[6] Blue text shows when anti-spam applications or laws were released. Red squares are the annual amounts stolen from Americans through phone fraud.[4]

While the spam volume of the USA is large, in terms of spam volume per capita globally, the USA is only number 8 (Figure 2). An effective solution to malicious spam must work globally, with the consideration that actual people, not robots, are often the ones making calls in countries where labor is cheap.

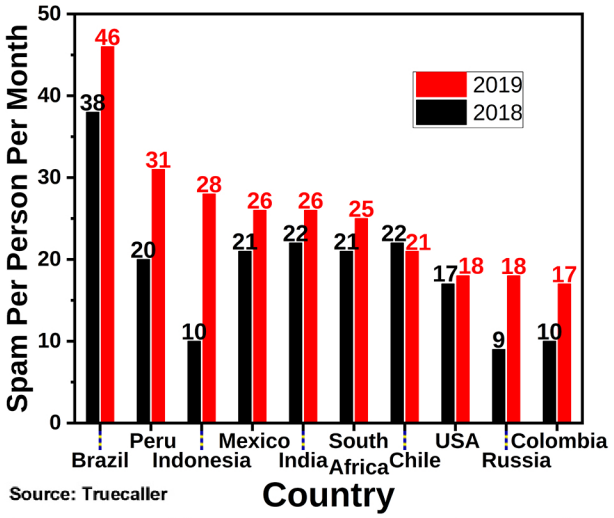

Figure 2. Monthly per-capita volume of spam calls per month in 2018.[7]

With this sort of financial incentive for bad actors to break the phone system, drastic measures must be taken. This proposal focuses on a free mobile application, RoboCash, that utilizes real-time fee-less refundable "NanoDeposits" to create unfavorable economic situations for those who create a high volume of malicious phone calls. The free app is simple, send all unknown phone numbers to voicemail, unless a NanoDeposit (e.g., $0.05) is received, in which case, let the call through. Your contacts are whitelisted so they may call you as usual. "NanoDeposit" is used in lieu of "microtransaction" due to the word's association with a small financial payment meant for goods/services. A NanoDeposit is meant to be an instantly refundable deposit as a sign of good faith. If the conditions are right, good actors (e.g. honest callers) will get their deposit back whereas bad actors (e.g. malicious spammers) will lose the majority of their deposits. The rise of open-source payment platforms has provided the fee-less, real-time digital cash that can scale to power the underlying financial backbone of such applications.

The Method

Consider Figure 3, a situation where Bob wants to call Alice, but Alice has RoboCash installed.

1. Bob is not on Alice's contacts list
   a. If Bob is on Alice contact's list, Bob's number is whitelisted and treated as a normal phone call.
2. Bob must pay RoboCash a NanoDeposit, meant for Alice, in order to ring her phone.
3. A timer starts on Alice's phone if she answers the call. The timer ends when the call ends.
4. Bob will get his NanoDeposit refunded in these cases:
   a. Call is ignored/not answered
   b. Call is received and call time lasts longer than 25 seconds
5. Bob will forfeit his NanoDeposit if:
   a. Alice answers the call and the call time is less than 25 seconds
      i. In this case, Alice gets 80% of Bob's NanoDeposit and RoboCash keeps the rest.

The time should be long enough that Alice has a chance to determine whether Bob is a bad actor or not, yet short enough that users are not forced to change typical phone call behavior. This paper estimates that time to be 25 seconds. It should be noted that if Bob is on Alice's contact list, the phone call proceeds as normal and the RoboCash escrow protocol is not needed. Furthermore, the NanoDeposit value and call time are tunable, thus can be adjusted. The app is merely a deterrent against bad actors. Any phone spam farms that attempt to work around this protocol will quickly find that this is not profitable, as the high volume of hang-ups per day, each costing a NanoDeposit, will eat into any fraud-derived profits.

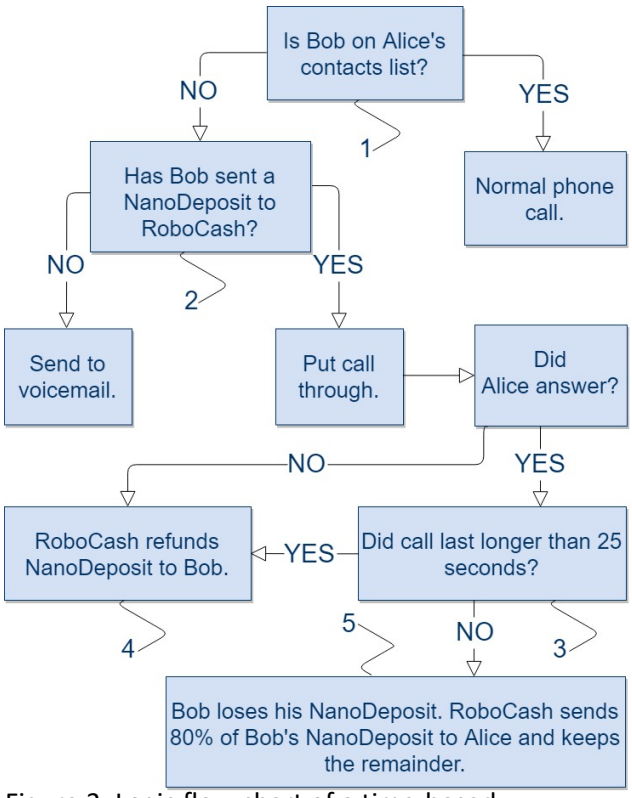

Figure 3. Logic flow chart of a time-based refundable escrow as an economic deterrent against spam calls.

Discussion

Installation of the RoboCash mobile application promotes awareness and education of these sorts of scams. The network effect[8] is imperative in order to make this app work on a meaningful scale. Figure 4 shows the expected outcome on fraud-derived profits. As the RoboCash network grows to include more and more users whom do not pick up calls from unknown numbers (unless paid a NanoDeposit). Thus, the pool of available devices for malicious parties to harass becomes smaller and smaller. In order to reach the threshold for the network effect and drive adoption, the app will be ad-free and free of cost for all users. There is no "buy-in" needed to use the app to block unknown calls or accept NanoDeposits. No identifying information, besides a phone number, is needed. RoboCash is designed to be as nonintrusive as possible in its role as an escrow wallet between Bob and Alice. RoboCash takes care of all the work for the users in an intuitive way. For example, when a user signs up with their phone number, RoboCash creates a unique wallet ID and attaches it to the phone number. When a balance is present, NanoDeposits are sent out for every call made through the RoboCash app's dialer. If no callee wallet is found, deposits are immediately refunded, so no loss ever occurs. This necessitates a social push for users, whom wish to call each other, to trade contact information and save the contacts to their phones, thus forgoing the chance of "false positives" (e.g. blocking legitimate callers). However, the beauty of RoboCash is that, unlike any other spam solution in existence, false positives are given a chance to bypass the filter using refundable NanoDeposits.

The only users that need to "pay-in" are those that plan to make cold calls. These entities can be primitively generalized as businesses. Paying NanoDeposits to reach users will become part of the customer acquisition cost of these businesses. This app promotes itself in two ways:

1. Indiscriminately prevent all robocalls, spam calls, and unknown numbers
    a. Solves the "false positive" problem, by giving genuine unknown calls a filter bypass protocol.
2. If an unknown call gets through, the user knows they are being paid for it and thus, are incentivized to answer their phone.
    a. If it is a robodial or spam call, or someone that does not immediately identify themselves, the user can simply hang up and pocket the NanoDeposit to punish the bad actor.

Point two brings up an interesting discussion. Over time, users will begin to associate incoming "unknown calls" with "NanoDeposits"; That is, they begin to associate unknown calls with money. This changes the dynamics of the existing

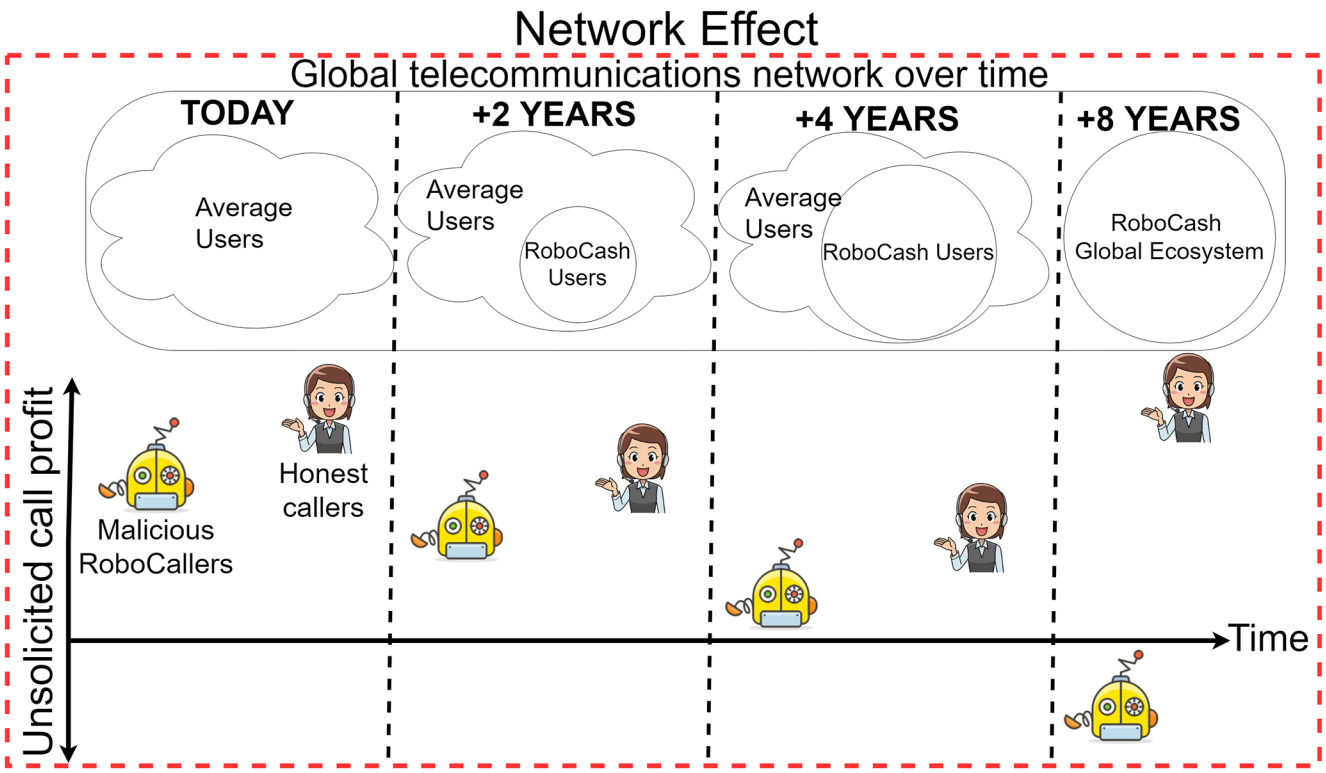

Figure 4. Diagram of the network effect. As the RoboCash network grows, less phones will answer calls from unknown numbers (unless paid a NanoDeposit). This gradually reduces the market size of victims for malicious callers until the market is no longer profitable.

telephone system by incentivizing users to answer calls from unknown numbers. This brings economic game theory to phone calls, which can be further gamified through creative business strategies.

Spam detection vs time-based refundable escrows

Part of the reason existing spam apps have had difficulty succeeding (Fig. 1) is that they rely on spam detection, which is computationally expensive and costly to scale. Due to these computational expenses, monthly fees are typically passed to users to offset costs. Charging users for a service adds a layer of financial friction, which slows user adoption and thus allows spamming to continue. RoboCash only asks 1 question, "Has this user's phone number received a NanoDeposit?". This Boolean logic reduces our computational time to the minimum needed, making RoboCash as scalable as possible.

The idea of "Payments at Risk" was first discussed by Rosenberg and Jennings over 10 years ago.[9] The idea was not pursued due to the lack of a real-time "micropayments" platform. Additionally, only 2 parties were involved in the Rosenberg method. The lack of a central wallet (such as how the RoboCash app is structured) means the Rosenberg method requires the receiving party (Alice) to perform a conscious judgement on whether the sending party's (Bob's) communication is "spam" and then perform additional actions to refund Bob. This puts unnecessary pressure on users. RoboCash uses a neutral time-based mechanism which does NOT require the user to perform any additional actions or thoughts than they would naturally do.

§ The primary requirements for a payment platform that can provide RoboCash with refundable NanoDeposits as an anti-spam mechanism are the following:

1. Fee-free
2. Real-time settlement
3. No fees to open new wallets
4. Scalable
5. Lightweight implementation
6. Attempts to be decentralized

Numbers (1-4) are obvious requirements for an application that intends to facilitate billions of call-based transactions between smartphones‡ every year. RoboCash can work with a "pure currency" distributed ledger. (5) Pure currencies offer a lightweight framework which allows RoboCash to operate on the user's phone without performing unnecessary work that drain the phone's battery. (6) A distributed ledger that attempts to increase its decentralized nature (e.g. have as many honest nodes routing transactions as possible) is more likely to continue operating with its user's best interests in mind. Fortunately, the rise of competitive payment platforms in recent years has produced one which fits all the requirements and will act as digital cash within the RoboCash protocol.[10]

Conclusions

Whereas previous anti-spam solutions have focused on the symptoms of spam calls through spam detection approaches; RoboCash focuses on the primary cause of the issue, economic incentives. These economic incentives are placed on the user's side (i.e. get paid to be part of the solution) and on the caller's side (i.e. lose money for spamming, get refunds for being honest) through a free mobile application. This innovation calls for a change in the way we allow others to contact us. It lets us properly value our own time, giving us financial control over our own data. Additionally, this removes regulatory pressure from common carriers by allowing users to decide what is "spam". If performed properly, this sort of implementation leads to awareness of the spam problem which further leads to a substantial reduction in the volume of phone spamming. Finally, the successful execution of this venture will serve as a proof of concept of the feasibility of fee-free, real-time, refundable NanoDeposits in transforming the way society interacts. Technology started this problem and technology shall end it.

Acknowledgements

To Dan Jenkins, an early advisor who recognized the potential of this application and was instrumental in pushing the pace of this endeavour.

Notes

§ Here, it is important to note that the decentralization scheme of a distributed ledger affects the latency and immutability of transactions with the ledger. These decentralization trade-offs are beyond the scope of this application and indeed, do not affect it, as RoboCash is ledger-agnostic and can use any distributed ledger which meets its needs.

‡ Smartphones are meant as a proof of concept that can be quickly deployed in the app store and can work on every app-store enabled device. The RoboCash protocol is robust enough to work over the existing telecommunications infrastructure without disturbing the underlying architecture. The payment platform simply acts as an independent second layer.

References

1. https://www.nytimes.com/2018/05/06/your-money/robocalls-rise-illegal.html.
2. https://www.theverge.com/2018/4/11/17223904/google-pixel-phone-app-spam-call-voicemail-update-android.
3. https://www.bbb.org/new-york-city/get-consumer-help/articles/the-nigerian-prince-old-scam-new-twist/.
4. K. F. Kok, Truecaller Insights, https://truecaller.blog/2019/04/17/truecaller-insights-2019-us-spam-phone-scam-report/, (accessed 27 May 2019).

5. https://www.cbsnews.com/news/sweepstakes-lottery-scams-cost-americans-more-than-100-million-in-2017/.
6. RoboCall Index. https://robocallindex.com, .
7. K. F. Kok, Truecaller Insights, https://truecaller.blog/2019/12/03/truecaller-insights-top-20-countries-affected-by-spam-calls-sms-in-2019/, (accessed 5 December 2019).
8. https://en.wikipedia.org/wiki/Network_effect.
9. J. Rosenberg and C. Jennings, The session initiation protocol (SIP) and spam, 2008.
10. C. LeMahieu, Nano: A feeless distributed cryptocurrency network.