Anatomy of a Robocall – Follow the Money

2021 NAAG Robocall Virtual Summit

September 8 2021

Matt Fischer, *Social Security Administration Office of Inspector General*
David Frankel, *CEO, ZipDX LLC*

Four General Categories of Phone Traffic

- Conversational
  - Family, friends, business-to-business
  - Human-dialed
  - Calls average several minutes
- Social Engineering
  - Special category of Conversational
  - Premeditated trickery to perpetrate fraud
- Auto-Dialed
  - Machine-dialed; detects human answer
  - Patches call through to call center agent
- Pre-Recorded
  - Very high volume – caller initially greeted by recording
  - Typically transferred to human agent if caller takes the bait (press 1)

Our Focus Today: Pre-Recorded Robocalls

- Server Computer does all the calling
  - Mastermind loads recorded (or artificial) voice
  - Cheap calling lists readily available on the internet
- Robocallers must pay for every answered call
  - But costs are a function of length of call
  - Robocalls on average are extremely short
  - Short calls are cheap; unanswered calls are free
  - $1,000 or less to make 1 million calls
- Once target takes the bait, transfer to live agent (the expensive part)
  - Callers make money by selling some product or service
  - Or worse, by stealing (and then reselling) identity or extorting money
  - If only a few dozen people succumb, that can be good money to the caller

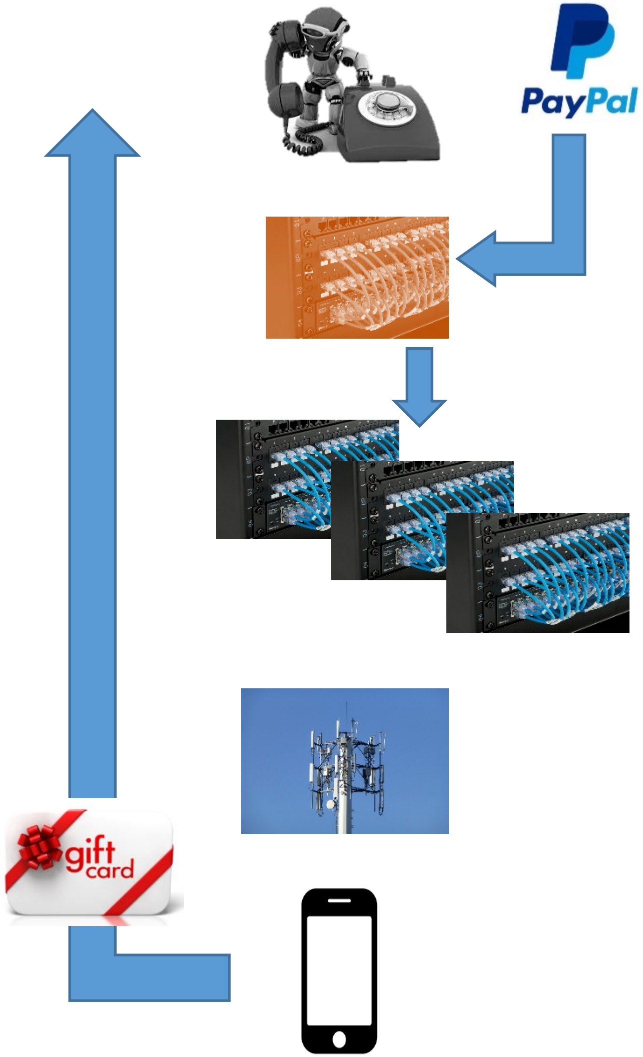
Charting Out The Robocalls

Notifications	Alerts specific to the called party, who usually welcomes the call (except perhaps for debt collection).		
Flight Cancellation	*School Closing*	*Prescription Ready*	*Fraud Alert*
Appointment Reminder	*Payment (Over)Due*	*Requested Callback*	*Utility Outage*
Placed by companies of all sizes, typically to parties with which they have an explicit relationship. Usually legal.			
Telesales	Promoting a product or service, often of dubious value. Caller claims consent from the recipient (perhaps in response to a web site visit); consent may be obtained unwittingly or not at all. May or may not be legal.		
Auto Warranty	*Health Insurance*	*Pre-Approved Financing*	*Employment*
Vacation	*Disability Claim*	*Home Security*	*On-Line Listing*
Usually placed by smaller companies but may reference brand names (Blue Cross, Medicare, Marriott). Mostly USA-based.			
Political / Charity / Survey	Not universally exempt. Callers often misrepresent themselves and have dubious messages.		
Fraud	Calls are blatantly fraudulent and illegal but prey on the vulnerable. Steal money or identity from the victim. Illegal.		
Government Imposter	*0% Interest Rate*	*Unauthorized Charge*	*Immigration Issues (Mandarin)*
Refund Owed	*Computer Virus*	*Utility Disconnect*	*Subscription Renewal*
Almost always placed by foreign scammers, but calls enter via USA gateways.			

How Did We Get Here?

- In the beginning, Ma Bell controlled every phone number and charged high rates to call across the country
- Advancing computer technology made phone equipment cheaper
- Now all phone signals travel as digital bits
- The 1996 Telecom Act opened telecom to further competition
  - Rates get pushed down even further
  - Anybody can be a phone company
- Historically, the phone companies did not police the use of their services
- Some telcos got sloppy and greedy, allowing high-volume calling & spoofing
- The Internet enables callers to operate from anywhere, anonymously

How it works: Calls & $$$ Follow Same Flow



- Caller (typically overseas fraudster or US-based telemarketer):
  - Fronts money for calling campaign
  - Spends $1,000 per million robocalls
  - Pays anonymously via PayPal
- Gateway or Origination Provider accepts payment to complete calls
  - Providers pay each other in turn as call proceeds; each keeps a margin
- Intermediate provider(s) pass calls along
- Phone companies say as far as they know calls are legal
- Calls reach potential victims; some press 1 to talk to an agent
- Human closer extracts $50 - $500 - $5,000 - $50,000 from vulnerable
  - Usually via gift cards or foreign wire transfer not traceable to recipient
- Good business for Caller/Fraudster and their provider!

Frequently Asked Questions

Q: How do robocallers get their phone numbers?

A: Often, they make them up. Imagine if the DMV let you draw your own plate. Some buy or rent thousands of numbers and cycle through them.

Q: Why do they ask for gift cards?

A: Gift cards are anonymous, untraceable, easy to convert to cash.

Q: How do they know my car warranty is expiring?

A: They don't. The recording tells a million people, "Your warranty is expiring." Some with expiring warranties press 1 (so do some others).

Q: My name is on the DNC list; why did they call me?

A: These callers are operating illegally. One more violation does not bother them.

Q: Why do they call me when I don't speak Chinese?

A: The computer calls millions of people. The ones that understand Chinese press 1. The others are just confused.

Q: Are the robocallers in this country?

A: Often they are not. The US-based phone providers that get paid to let these calls in need to stop doing that.

Q: The caller-ID said they were in Indianapolis. Can you go arrest them?

A: Usually the caller-ID is made up. The caller could be in Indiana or India.

What Can We Do About It?

- Callers are often hard to identify or unreachable (non-US based)
- Always a US-based telecom provider that accepted payment for the call
- Providers violate FTC's TSR, FCC's TCPA & other state/federal laws:
  - "Assisting and facilitating" those engaged in deceptive/abusive practices (TSR)
  - Failing to ensure its services are not used for unlawful traffic (TCPA)
  - Participating in another party's deceptive act or practice (state UDAP statutes)
  - Potential criminal statutes such as wire fraud and money laundering
- Trace back a few examples to find responsible provider(s)
- Obtain Call Detail Records to determine extent of the provider's involvement
  - Determine average call duration & distribution; Caller-ID values
  - Analysis can reveal millions of obviously illegal calls (violations)
- Hold these providers accountable; enjoin them from making more calls

Holding Providers Accountable

- Where there’s smoke, there’s fire.
  - Some providers protest that the illegal calls are “exceptions”
  - Investigations prove otherwise
- January 2020: SSA, DoJ v. Global Voicecom and TollFree Deals
  - TollFreeDeals transmitted an estimated 143 million fraudulent robocalls on behalf of [a] single India-based co-conspirator during May and June of 2019. Of those calls, an estimated 20% were Social Security imposter calls, 35% were loan approval scams, and 14% were Microsoft refund scams. The remaining calls were a mixture of IRS imposter, U.S. Treasury imposter, miscellaneous tech support imposter and other schemes.*
  - Court issued a Permanent Injunction, effectively shutting down TollFreeDeals.
- April 2021: Vermont AG v. Strategic IT Partner*
  - In one day alone, SITP routed hundreds of thousands of fraudulent robocalls from foreign customers to the U.S., including thousands to Vermont.*
  - SITP must now vet its customers and monitor their call records for short-duration traffic and must pay a fine.*

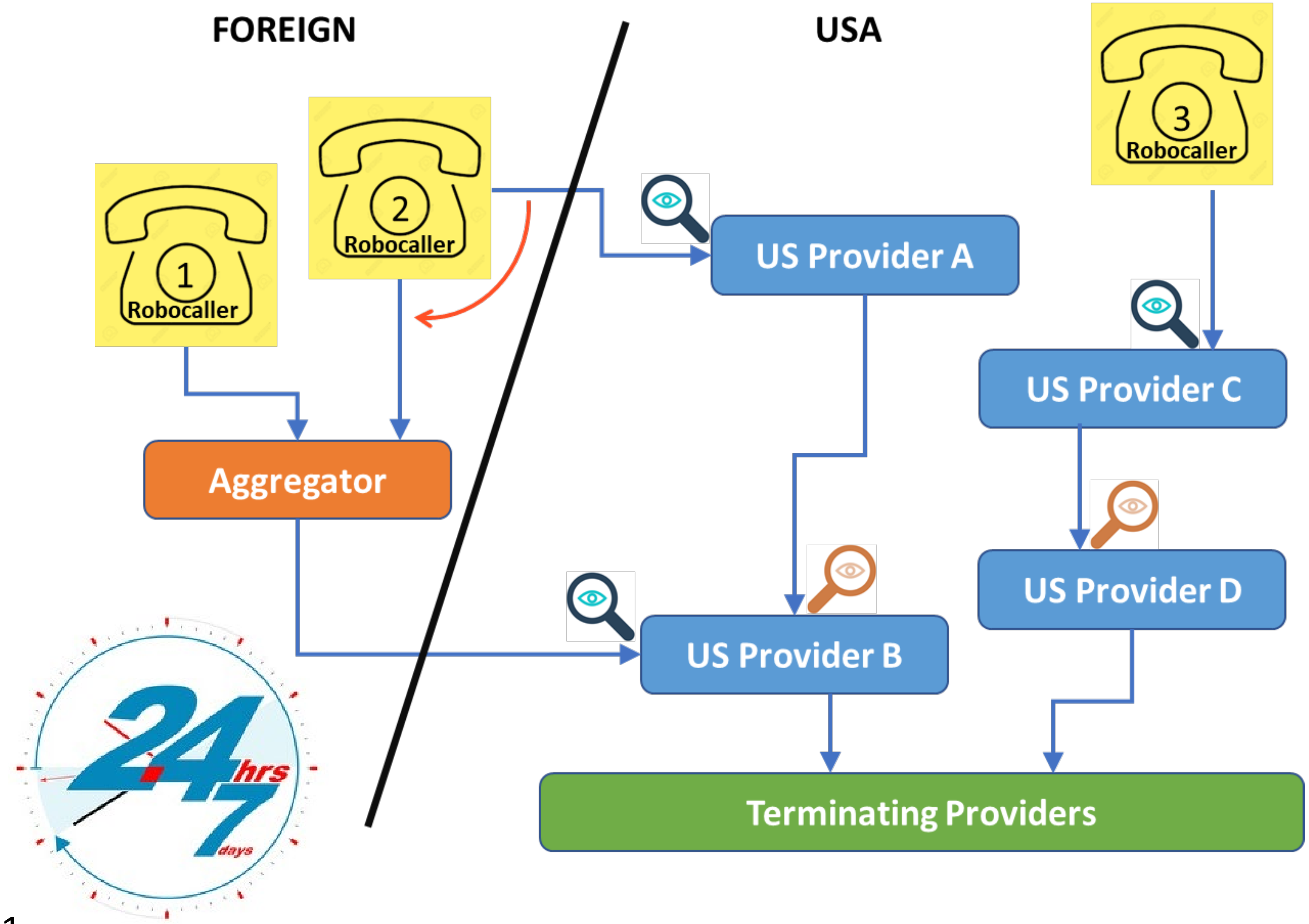
* From court filings and press releases related to the cases

A ~~Twelve-~~ Three-Step Program

1. Ideally, providers that get paid to enable these calls would stop
   - Some engage knowingly, soliciting illegal traffic with thinly-veiled advertisements
   - Others look the other way; claim they had no way of knowing customers were fraudsters
   - For many, if they cut off this traffic, they will have no other revenue
2. Intermediate providers are complicit if they do business with enabling providers
   - Intermediate providers need to vet new customers and proactively monitor traffic
   - Short duration traffic with many distinct caller-IDs must be promptly investigated
   - Refuse calls until the originator/gateway supplies a compelling explanation
3. Regulators and enforcers must step in where industry falls short

- All this must happen DILIGENTLY and QUICKLY to stay head of the fraudsters.

Closing the Floodgates



- Gateways & originators must scrutinize their traffic; downstreams must watch their upstreams (esp. dialer traffic)
- SSA assists w/ cases involving SSA accounts and phone numbers
- ZipDX makes CDR analysis tools available to providers and enforcers
- Millions of calls can be analyzed in seconds
- Illegal traffic comes into focus
- Analyze traffic nightly or even more frequently
- Rapid response is required to stop perpetrators from reinventing themselves

One Day’s Traffic for “RoboCalls-R-Us”

Customer (Upstream)	Call Count	Dialed #s	ANIs	Calls Per ANI	<= 60 Secs	> 2 Mins	>2 Min %	ACD (sec)
Caller A	168,424	155,396	46,342	3.63	97.7%	1,122	0.7%	16
Caller B	3,878	3,130	1,001	3.87	46.4%	1,354	34.9%	203
Caller C	2,569,787	2,474,211	1,678,219	1.53	99.1%	6,647	0.3%	15
Caller D	170,322	138,791	26,573	6.41	95.5%	3,440	2.0%	24
Caller E	2,550	1,992	1,501	1.70	68.5%	516	20.2%	177
Caller F	116,279	107,820	50,034	2.32	98.6%	293	0.3%	15
TOTAL	3,031,240	2,881,340	1,803,670	1.68	98.5%	21,790	0.7%	15

Conversational Calling: 20% or more calls at least two minutes; ACD > 3 minutes (B)

Robocalling: 90% of calls are less than one minute; ACD < 1 minute (A, C, D, E)

Calls Per ANI: Less than 10 indicates random spoofing or snow-shoeing

Vendor (Downstream)	Call Count	Dialed #s	ANIs	Calls Per ANI	<= 60 Secs	> 2 Mins	>2 Min %	ACD (sec)
Provider W	1,423,777	1,395,206	894,560	1.59	98.3%	3,628	0.3%	16
Provider X	744,617	689,563	512,202	1.45	97.2%	1,142	0.2%	18
Provider Y	519,239	476,780	307,339	1.69	99.2%	3,877	0.7%	15
Provider Z	343,607	319,791	89,569	3.84	95.5%	3,440	1.0%	24
TOTAL	3,031,240	2,881,340	1,803,670	1.68	98.5%	21,790	0.7%	15

- Call Detail Records (CDRs) reveal nefarious calling
- This provider has CDRs for their customers and can discern concentrated dialer (short-duration, robo) traffic

- The provider’s downstreams (vendors) can see similar patterns
- Investigations to date reveal certain providers choose to deal almost exclusively in this traffic, with minimal vetting and monitoring
- Providers must look at their own traffic before the enforcers come calling.

Do-It-Yourself

- This analysis can be done with open-source database software (MySQL)
- CDR table contains:
  - dialed – 10-digit NANP called number
  - ani – digits supplied as the caller-ID
  - duration – duration of the call in seconds
  - customer – identifier for the customer
- Process 5 million CDRs in under a minute
- Rent a cloud server if you don't have your own
- Analyze traffic nightly or even more frequently
- Demand immediate, detailed explanation for all suspicious traffic
- Stop traffic if no credible explanation within 48 hours

```
SELECT
  customer,
  COUNT(*) AS calls,
  COUNT(DISTINCT ani) AS uniqanis,
  ROUND(COUNT(*)/COUNT(DISTINCT ani),2) AS cpani,
  COUNT(DISTINCT dialed) AS dialdns,
  ROUND(SUM(duration <= 60)/COUNT(*)) AS plt60,
  ROUND(SUM(duration > 120)/COUNT(*)) AS pgt2min,
  ROUND(SUM(duration)/COUNT(*),0) AS acd
  FROM cdrs
WHERE duration > 0 /* only analyze answered calls */
GROUP BY customer WITH ROLLUP;
```

In Closing…

- What questions, comments and ideas do you have?