



Defeating Phone Scams with Conversational AI

Disclaimer

This presentation deck contains confidential and proprietary information of Apate.AI Pty Ltd (ACN 674 088 87) intended solely for the recipient's use. The recipient has not signed a non-disclosure agreement, but by accessing this presentation deck, you acknowledge and agree to treat all information herein as confidential, and you are expected to maintain the confidentiality of the information.

Unauthorised disclosure, copying, distribution, or use of any information contained in this presentation deck is strictly prohibited. If you are not the intended recipient, please notify the sender immediately and delete this presentation deck without making any copies or disclosing its contents.

The information provided in this presentation deck is for informational purposes only and should not be relied upon as the sole basis for investment, business, or financial decisions. While reasonable care and diligence have been exercised in the preparation of this presentation deck, no warranty or guarantee is provided as to the accuracy, completeness, or reliability of the information.

Recipients are encouraged to conduct their own independent analysis, due diligence, and to seek professional advice before making any decisions based on the information provided herein. By using this presentation deck, you agree to hold harmless the authors, contributors, and any affiliated parties from any liability arising from your use of or reliance upon the information contained herein.

Intro

The global phone scam challenge is growing exponentially

 A quarter of all unknown calls are scams or fraudulent

Scammers make 70 million calls globally every single day

- this costs victims billions of dollars annually;
- degrades consumer trust; and
- damages brand reputations.

Our mission is to break the business model of scammers to beat them at their own game.

Context

Scale of the problem in Australia

\$3+ Billion Total Combined Losses ►

Reported to Scamwatch, ReportCyber, IDCARE, Australian Financial Crimes Exchange and government agencies.

COMMUNICATIONS ALLIANCE LTD INDUSTRY CODE C661:2022 REDUCING SCAM CALLS and SCAM SMS 2022

Text Messaging



\$28 million
reported lost

Calls



**\$141 million
reported lost**

Email



\$77 million
reported lost

Internet



\$74 million
reported lost

Social Media



\$80 million
reported lost



◀ \$141 Million Reported Lost from Phone Calls in 2022

COMMUNICATIONS ALLIANCE LTD INDUSTRY CODE C661:2022 REDUCING SCAM CALLS and SCAM SMS, 2022

Context

Reported cases and loses in the US and Singapore

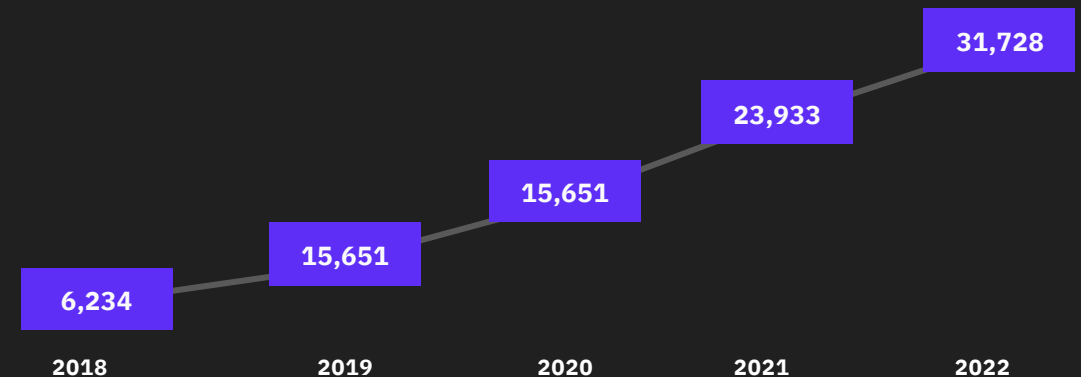


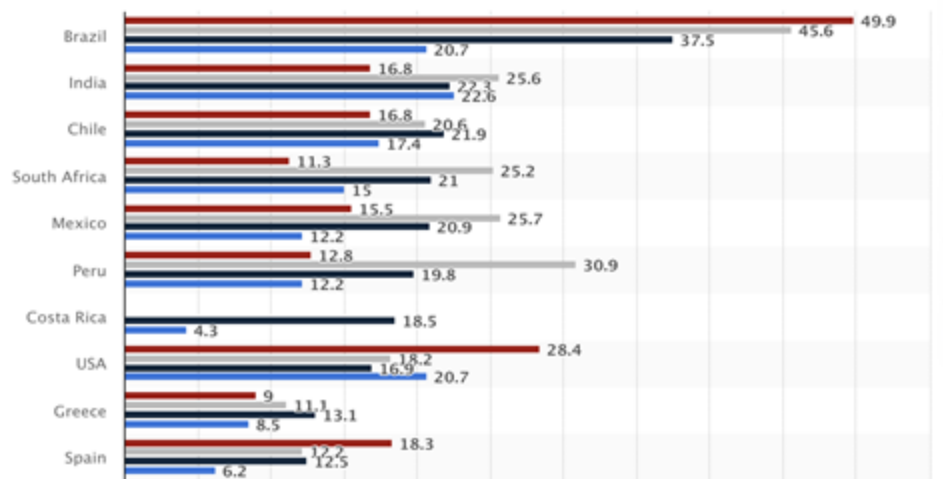
◀ **\$8.8 Billion Reported Loss in US in 2022**

FTC Report 2022. TrueCaller Data 2022

An ever-increasing number of cases in Singapore

Singapore Police Force Report, 2022



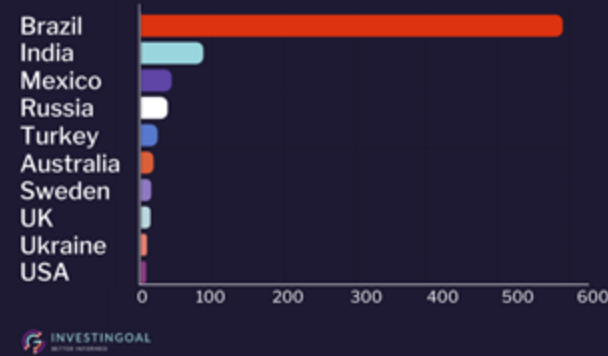


▲ Number of Spam Calls per User per Month

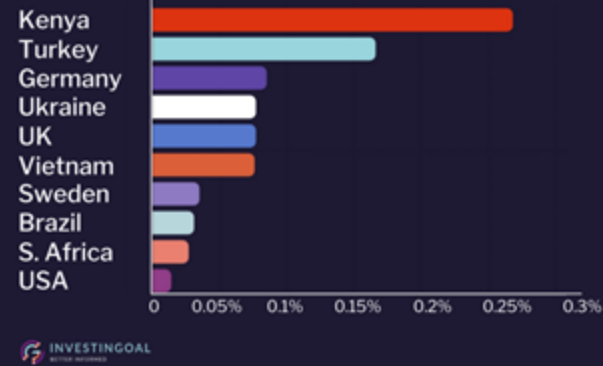
Petroc Taylor, Statista, 2023

Average monthly number of spam phone calls per user in selected countries from 2017 to 2020, 2023

No. of scams per 1,000 people in 2021



GDP loss due to scams (%)

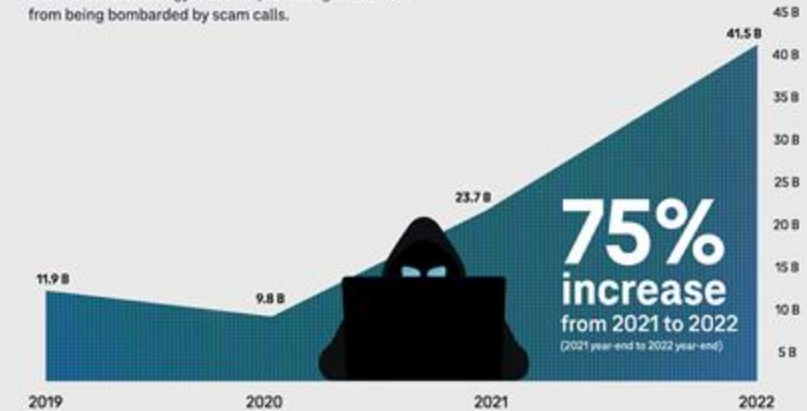


Constantly evolving and improving scam attempts

T-Mobile Report US, 2022

Scam Call Attempts Reached Record Highs

Scam block technology is vital in protecting consumers from being bombarded by scam calls.



A Global Problem

Why are scams are still a major challenge

Root Causes of Scams

Although billions of dollars are spent on scam detection and prevention, billions of dollars are still lost to scammers.



Technological Aspect

Simple to execute, VoIP makes it easier, Hard to upgrade telecommunications provider infrastructure



Social Aspect

Mimics real life stories (e.g. ATO), Preys on human emotions and fears, Targets the most vulnerable people



Monetary Incentives and Financial Challenges

High gain to cost ratio for scammers, Hard to recover scammed money, Costly infrastructure change



Prevention and Enforcement Challenges

Scams originate from foreign jurisdictions, Detection mechanisms overwhelmed, Not enough timely threat intelligence

“

Behind the mind-boggling statistics are real human beings, who are crippled by debt, traumatised by their ordeal and are stuck wondering how to rebuild their lives.

”

Nerida O'Loughlin, Australian Communication and Media Authority (ACMA)
Chair, May 3rd 2022.

Our Mission

**To break the scammers'
business model, globally**

Content



— 01

What is Aplate.AI?

The Aplate Solution

How it Works

— 02

Who is Aplate.AI for?

Products

Opportunity

— 03

Traction

Progress & Achievements

Technology Roadmap

— 04

Team

Founding team and advisors

University Support

— 05

Ask

Seed Investment

Use of Funds

— 06

Appendix

Financial Forecast

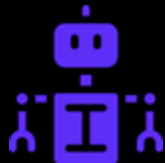
Technology

01

What is Apate.AI

What is Apate.AI

Apate offers the perfect Victim Chatbot



Our Victim Chatbots are engaging scammers for up to 50 min

How

LLM fine-tuned on call transcripts

- Scam transcripts sourced from multiple channels
- Youtube “scam baiters” and reddit enthusiasts

Deep analysis of scammer methods

- To identify effective strategies to engage scammers
- We draw insights into scammer methods
- Hard to obtain, sellable info on current scams

Early scam detection and alerts

- Trained ML on calls’ meta-data for scam identification
- Multi-platform scam detection for extended alerting

Optimised AI for longer conversations

- Based on success or failure of current strategies.
- Reinforcement learning on call-length and dialogue of self-play.

Features

Diverse Personas

Pre-Trained on hundreds of hours of real conversations

Scam Baiters Minded

Conversation Memory, Trained Objective Function, Shared Mental Models

Reinforcement Learning

Over 1000 hours and counting of real scammers conversations

AI Voice Cloning

Supports convincing Victim Chatbot voices

Multi-Lingual

English, Mandarin, Egyptian, German, Russian, Arabic, French and more

Enhanced Conversation Features

Human-like voice, realistic interplay between interlocutors with injection of disfluencies, emotions, backchannelling and minimised speech delays.

Scam Fitting

Bot derives intent of the scammer and reacts in a way to deceive them

Context and Category Awareness

Probabilistic models built on the fly for each category of scam call, inferring conversation status and delaying transitions to the next stage of the scam plot

Continuous updates

Containerised solution flexibly adapted, and updates instantly deployed

Products

APATE AI.Callee

Calls are redirected to Victim Chatbots with virtually an infinite number of Profiles/Personas

APATE Insights

Accurate and timely Threat Intelligence for enterprise and government agencies

A Novel Approach

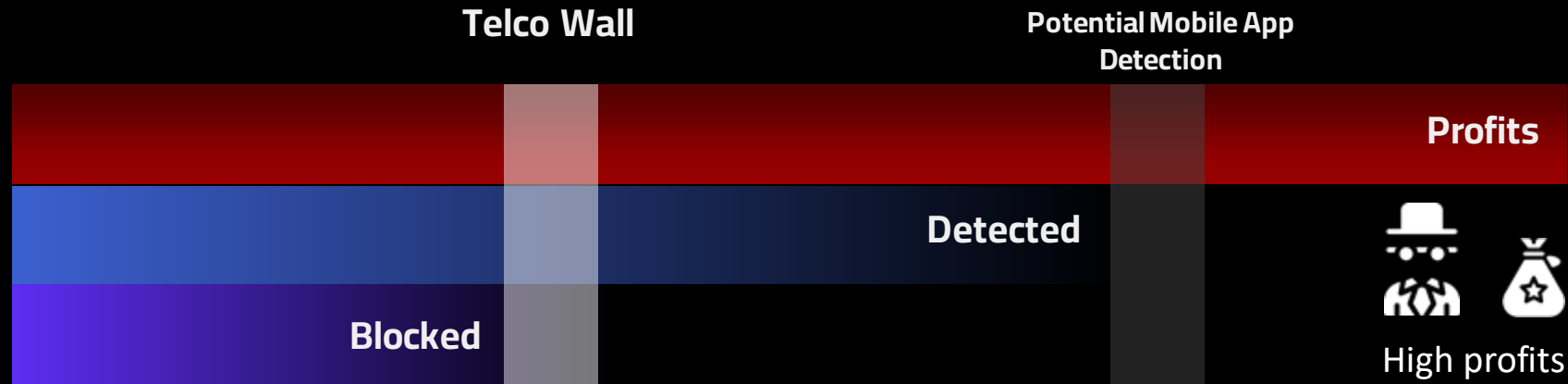
Breaking the business model of scammers

EXISTING APPROACH

(REACTIVE)

Detect, Filter and
Block

Scam calls

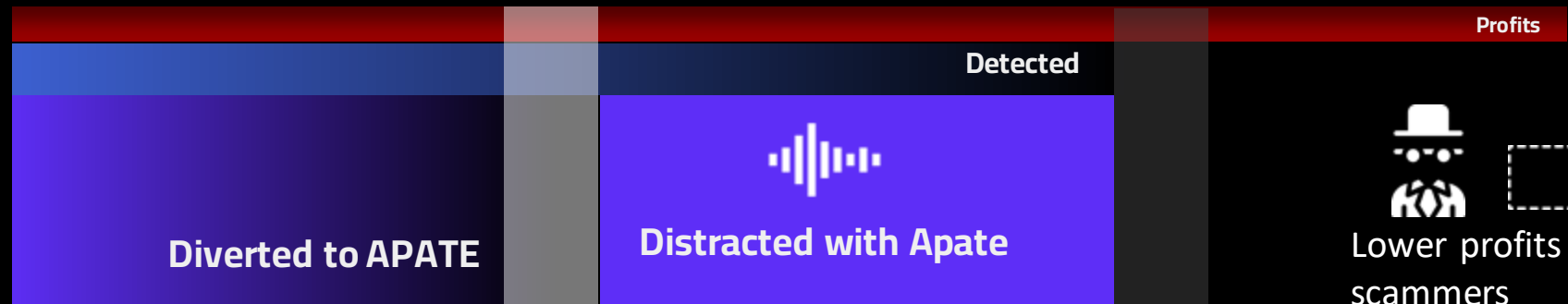


APATE APPROACH

(PROACTIVE)

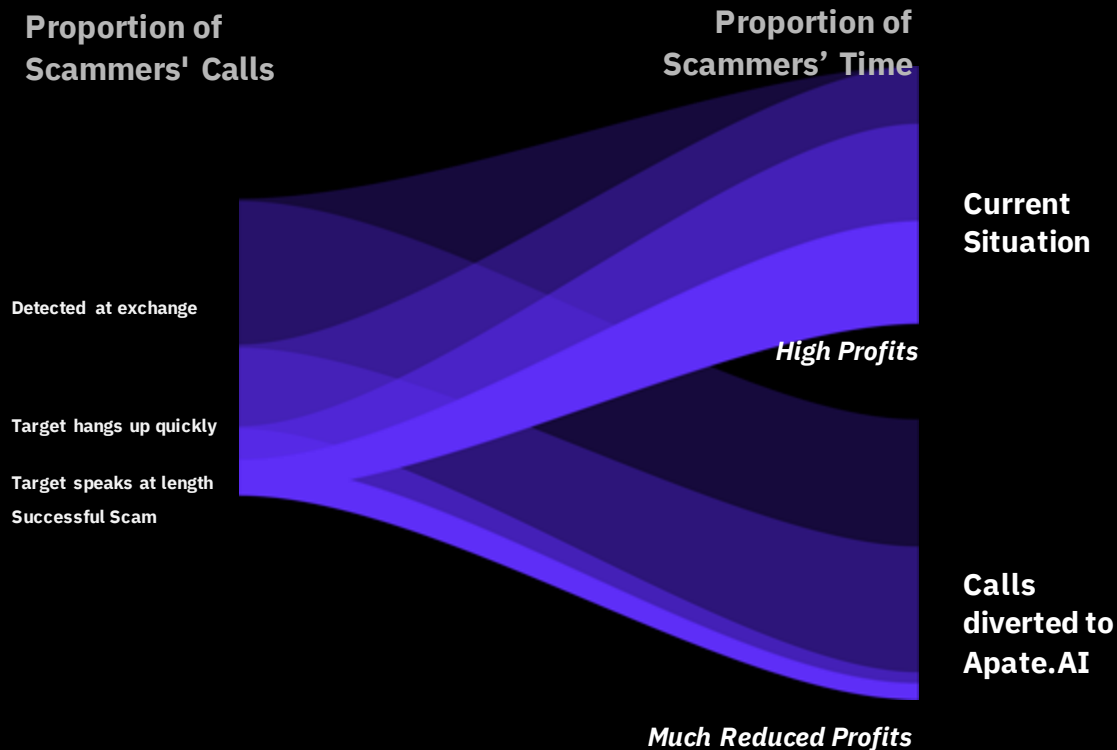
Divert, Distract
and Disrupt

Scam calls



Apate.AI

From reactive to proactive scam defense



Current (*Reactive*) approach to protect phone service users from scammers

- Educate users / share best practices
- Detect/Filter/Block some scam calls
- End users solutions (Mobile apps to detect scam, notifications based on callers reputation)
- Scam intelligence reliant on crowd- sourced victim reporting

- ▶ Detect, filter & block scam calls on telco (in-house and vendors)
- ▶ Educate consumers - augment consumer phone with a notification that a call may be a scam (Robokiller, Hiya, TrueCaller, etc.)
- ▶ Intelligence is crowd-sourced post scam losses or reports

Apate.AI (*Proactive*) approach

- Conversational AI trained to imitate plausible, realistic scam victims
- Optimized to maximize scam call duration
- Early threat intelligence of "scampaigns"
- Deployable at any Telco network, preventing scammers from reaching actual phone service users
- Agnostic to the location of the scammer and adaptive to the location of the network to protect (Multi-lingual, multiple dialects)

- ▶ Disrupt & Deter scammers. Respond to and Prevent new scams.
- ▶ A network free of scam calls
- ▶ Extracts intelligence in real-time from scammer conversations

A feel of what Apate bots sound like

Edno



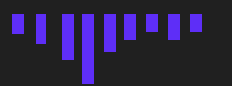
British, 65 Year Old Male
Scam Category: Gift Card
Overall Emotion: Collaborative
[Have a listen](#)
[Transcript](#)

Edna



Australian, 47 Year old Female
Scam Category: Amazon Purchase
Overall Emotion: Aggressive
[Have a listen](#)
[Transcript](#)

Mary



Australian, 50s Year Old Female
Scam Category: Investment
Overall Emotion: Skeptical
[Have a listen](#)
[Transcript](#)

Ibrahim



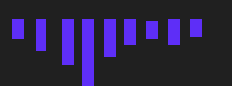
Egyptian, 62 years old Male
Scam Category: Netflix Payments
Overall Emotion: Collaborative
[Have a listen](#)
Transcript (In Egyptian)

Ibrahim



Egyptian, 62 years old Male
Scam Category: Netflix Payments
Overall Emotion: Collaborative
[Have a listen](#)
Transcript (in Egyptian)

Brad



American, 25 years old
Scam Category: Social Security
Overall Emotion: Cool, chilled
[Have a listen](#)
[Transcript](#)

02

Who is Apate.AI for?

Products

Core customer solutions

Apate AI-Callee

- Calls blocked to be redirected to Apate AI-Callee (SIP or WebRTC)
- Guaranteed Minimum #min per call
- Multilingual Bots to be connected
- Targeted threat intelligence extraction via customisable dashboard and API calls

Apate Insights

- Enterprise and Government agencies receives near real-time notification of scam campaigns
- Threat intelligence includes scam categorisation, scam stages/scripts and scammer narratives
- Periodic (daily/monthly) detailed reports via web portal dashboard and APIs
- Global intelligence sublicensed for all impersonated organisations across

[Solutions](#) [Pricing](#) [About](#) [Sign up →](#)

Telco offer

Apate AI-Callee

\$40K

per month to make phone scams ineffective in your network using Apate AI scam victim

- ✓ up to X calls
- ✓ unlimited AI personas
- ✓ >5 mins of calls

★ **Bonus:** Scam near real-time notifications up to 10 entities

Get AI-Callee →

Org offer

Apate Insights (Targeted)

\$2K

per month to continuously monitor who and how targets your organization (1 entity)

- ✓ Near real-time notifications
- ✓ Scam intelligence
- ✓ Scam analytics
- ✓ Detailed reports

Get Insights →

Org and Gov offer

Apate Insights (Global)

\$10K

per month to understand global scam market (all scam campaigns)

- ✓ Near real-time notifications for selected entities
- ✓ Scam intelligence
- ✓ Scam analytics
- ✓ Detailed reports

Get Insights →

Who Benefits

Personas for our Products

Apate AI-Callee



Telecommunication Providers

Globally, Telecommunication providers spend billions on scam call detection, blocking and filtering.

Legislation requires Telcos to reduce scam calls (e.g., Australia C661;2022 Rules from ACMA “Reduced Scam Calls Code”, Operation Stop Scam Calls 2023 FTC and attorneys general from 50 states, TRACED Act 2020, etc.)

- ▶ With Apate, increased customers trust and reduced expenditures on detection and blocking

Rules also require telecommunication providers to assist their customers in proactively managing scams and are required to share information about scam and report scam campaigns

- ▶ With Apate, Efficient Intelligence collection and real-time reporting of “Zero-day” Scam intelligence

Apate Insights



Enterprise and Government

Impersonated businesses and government agencies currently know about campaigns targeting their customers only too late, mostly relying on crowd-sourced intelligence from user reports or scam loss reports/complaints.

- ▶ With Apate, real-time and accurate intelligence collection for timely response and prevention of loss. Insights into scammer methods and targets.
- ▶ Reduced effort by fraud teams seeking hard to obtain intel on current “scampaigns”
- ▶ Less scam complaints and mitigation work






Retail Consumers

Consumers are all vulnerable to scammers. When not falling for scams, consumers are spammed by undesirable calls, feeling vulnerable and **losing trust** in their phone network and service providers.

- ▶ With Apate, a greatly reduced number of scams, consumers regain trust facilitating increased use and sharing of positive sentiment.
- ▶ Consumers receive accurate information about current “scampaigns” and receive details on how to avoid falling victim

Total Addressable Market

Scale of the opportunity

Apate AI-Callee		Apate Insights	
 Telecommunication Providers	 Enterprises	 Government	
<p>Over 25K Wireless telecommunication carriers globally. In U.S., 30 Telcos listed by CTIA (Cellular telecommunications and internet association) have their own infrastructure</p> <p>On average, 2 to 3 major telecommunication providers per country, all subject to anti-scam regulatory requirements (E.g., ACMA in Australia, FCC in US, ComReg in Ireland, OfCom in UK, MCIT in KSA, etc.)</p> <p>The GSMA, unites more than 750 operators with almost 400 companies in the broader mobile ecosystem.</p> <p>The top 100 largest telecom providers and operators, including Verizon, AT&T, Deutsche Telekom, T-Mobile, NTT, Vodafone, STC and América Móvil, generate over \$1.7 trillion of revenue each year and employ more than 4.5 million people around the world</p> <p>The global fraud detection and prevention market size was valued at USD 25.67 billion in 2022 and is expected to grow at a compound annual growth rate (CAGR) of 17.6% from 2023 to 2030</p>	<p>Consumer protection</p> <p>FSI regulators, ASIC (Australia), ACMA, The Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA) in US, Financial Conduct Authority in UK, The Federal Financial Supervisory Authority (BaFin) in Germany, etc. mandate active defense and prevention against scam related threats to customers.</p> <p>Non-FSI enterprises with B2C touch points are targeted by scammers across industry verticals including include logistics, media and entertainment including big tech etc. These companies have duty-of-care to advise of "scampaigns" targeting their organisations and customers</p> <p>The global threat intelligence market size was valued at USD 4.24 billion in 2022 and is projected to grow from USD 4.93 billion in 2023 to USD 18.11 billion by 2030</p>	<p>Australia</p> <p>Nat Sec agencies – ONI, ACSC, ACMA, ACCC (National Anti Scam Centre)</p> <p>Government agencies – ATO, Services Australia, Services NSW, etc, ACCC/ ScamWatch, Department of Infrastructure Transport, Regional Development, Communications and the Arts.</p> <p>Global</p> <p>Government and national security agencies across the world have mandates to be cognizant of current threats impacting their citizens. Similar to Australia, international machinery of government is siloed and there are 2-3 primary agencies and a range of secondary agencies seeking scam intelligence in each jurisdiction.</p>	

03

Traction

Key Partners

Saudi Telecom

The logo for Saudi Telecom Company (stc) in white text on a dark blue square background.

Heads of Agreement to quantify impact on scammers and demonstrate real-time threat intelligence. ~USD\$450K over 12 months

TPG Telecom / CBA

The logo for TPG Telecom, featuring the lowercase letters 'tpg' followed by the word 'TELECOM' in all caps, with five dots above the 'COM'.

Trial with support from the AEA and Industry Growth programs

Deutsche Telekom



Proof of concept with medium scale, multi-horizons collaboration

ONI



Sponsor and Funder of the Research behind Apate. ~USD\$450K

NVIDIA



Apate selected for Nvidia Inception Program. Free use of NVIDIA HPC, NVIDIA AI, Free cloud credits, on-going Discounts on NVIDIA services

Octo.AI



Annual support with financial credits and custom low latency deployment

POC Performance

Preliminary Results with Early Design Partner

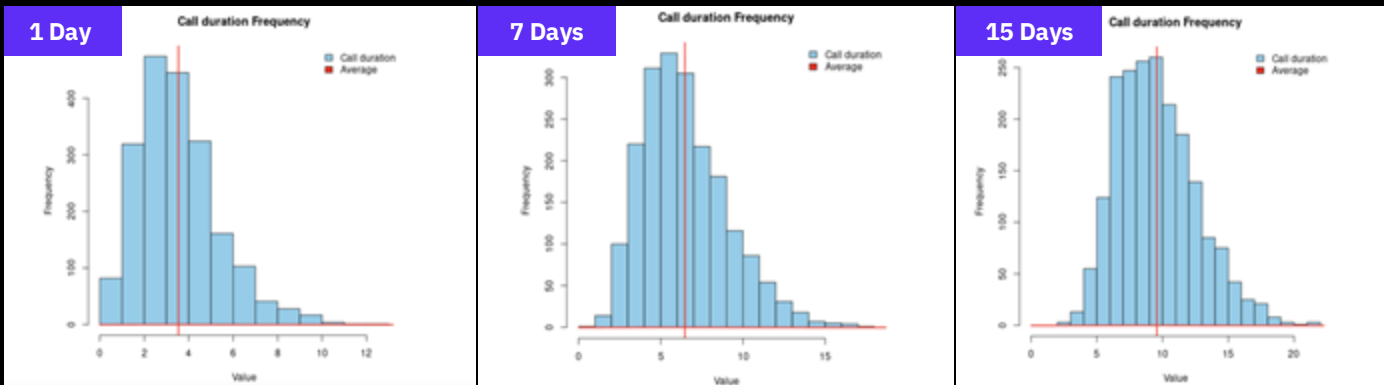


Data

110 hours of Real Human (Scam baiters) Scammer Interactions

~14K phone scam calls over 3 months period

- Generated: 91840 min (1530 hours) of conversations between Victim Chatbots and Scammers
- Average call duration 6.56 min
- Reinforcement Learning (No-Yes): 620 – 910 hours



◀ **Average call length increased from 3.5mins to almost 10 minutes over the course of 15 days training**

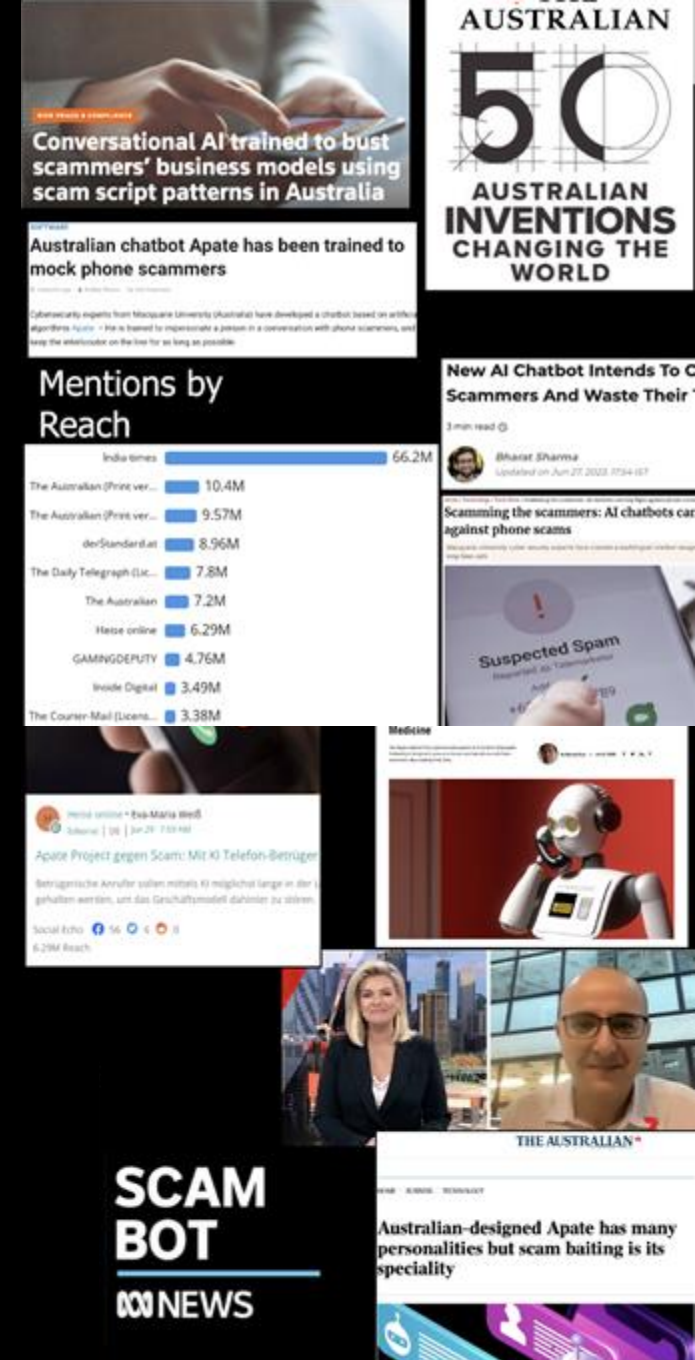
	Horizon 1: Jan 2024 – June 2024			Horizon 2: July 2024 – Sep 2024			Horizon 3: Oct 2025 onward		
Scope	Preparing for scaled deployment in the context of live scam calls			Scaled deployment POC			Commercial customer		
	Complete development of our current prototype, adding scaling capabilities, establishing cost saving methodologies, refining pipeline design, and developing data insight models and infrastructure, all in the context of moderate scale conversations with scammers			Deployment at medium scale to demonstrate obtaining real-time business intelligence and quantify impact on scammers. Core reductions in running costs demonstrated and further refinements made. Ongoing innovation in core pipeline capabilities and adaptive AI			Deployed at full scale with live business intelligence and significant impact on scammers. Ongoing collaboration on pipeline/bot optimisation for further improvements to costs and effectiveness in the face of inevitable behaviour changes from scammers		
Products/ Outcomes	Proof of Concept <ul style="list-style-type: none"> - Scaling capabilities - Cost saving methodologies - Adaptive AI testing - Data insight capabilities 			<ul style="list-style-type: none"> - Live deployment monitoring and controls - Live scam insight monitoring and alerts - Novel cost reduction methodologies (eg: caching utterances) Optional: Scam intelligence			<ul style="list-style-type: none"> - Significant impact on scammers including significant reduction in successful phone scams to customers. - Low-cost use of Apace services discounted markup on cost. - Ongoing Apace R&D in pipeline/bot adaptation and scam monitoring 		
Commercial	1,000 daily calls, 10c per minute			10,000 daily calls, 4c per minute			100,000 daily calls, 0.5c per minute		
	TTS	75%	Realistic voice generation	TTS	57%	Discounted realistic voice generation	TTS	59%	Custom voice generation
	STT	19.5%	MZ Azure speech recognition	STT	41%	Discounted speech recognition	STT	30%	Custom speech recognition
	AI Bot	4.0%	GPT 3.5 large language model	AI Bot	1.5%	GPT 3.5 large language model	AI Bot	9%	Custom speech recognition
	Cloud	1.5%	Azure VMs	Cloud	0.5%	Azure VMs (economies of scale)	Cloud	2%	Discounted Azure VMs
Financial	Platform		USD\$10,000 per/month	Platform		USD\$15,000 per/month	Platform		USD\$20,000 per/month
	Personnel		To be co-defined	Personnel		To be co-defined			
	Total		To be co-defined	Ask		To be co-defined	Total Cost		USD\$25,000 per/month

Sample Design Partner Program



Achievements

- Generous **Funding from the Office of National Intelligence (ONI)**
- Recognised as **Top50 Australian Innovation of the year 2023**
- Founder recognised as **Top100 Inventors 2023**
- Awarded **First prize** of the Incubator's Researchers' IMPACT Program
- **Advanced PoC partnership trials** (12 months + Commercial agreement ~400K USD per year) with STC (KSA). Engagement with Deutsche Telekom (Germany) and TPG Australia
- **Over 15K requests** from end users worldwide, and **media coverage reaching over 150M individuals** (Reuters, National TV, India Times, BFM-TV, HeiseOnline, the Australian Podcast) since public launch (July 2023)



Technology Development Roadmap

What we've achieved so far (TRL 5)

- SIP and Web RTC Integrated
- **LLM/GenAI Based Bots**
- **Diverse AI Personas**
- Tailored High-Quality “victim” Voices
- Post Call Intelligence
- Seed data from scam calls on
- Conversation control heuristics
- Multi-Lingual bot (English (3 variants), Mandarin, Egyptian, German, Russian, Saudi, French)
- Scalable Pipeline
- Reinforcement Learning Enabled

Future Development

- Run Cost Reductions (Fraction of a cent/min)
- Near Real-Time Threat Intelligence
- Global Fraud and Scam Alerting
- Language Detection and Cross-Language models
- Automated Personas Generation
- IM (WhatsApp, signal, etc.) and VoIP support

04

Team

Core Team

Born out of Macquarie University supported by the Office of National Intelligence (ONI)

Dali Kaafar



Founder & CEO
Professor of Cyber Security
Executive Director Cyber Security Hub

Ian Wood



Co-Founder
Researcher and AI / NLP
Specialist

Michal Kepkowski



Co-Founder & Chief Architect
Software Architect and DevOps
specialist

Nardine Basta



AI Researcher
Post Doctoral Researcher
Cyber Security and AI

Connor Atkins



Researcher
PhD candidate Conversational AI

David Plisek



Co-Founder & Operations
Serial Founder and Cybersecurity
Professional

Advisors

Apate has assembled a world-class team of Advisors to help build, support, and grow



JOSH KENNEDY-WHITE
(CO-FOUNDER)

- Commercialisation Advisory



NILOUFER SELVADURAI

- Legal Advisory



DAN JOHNSON

- Research Partnership Advisory

Technology Advisory Board

Ersin Uzun (Leading Researcher, Ex-Innovation Manager XEROX PARC)

Simon Kriss (Chief Innovation Officer, Customer Experience Innovation Institute)

Cameron Esdaile (VP of Technology and Innovation, ThousandEyes - CISCO)

University Support

**Macquarie
University is an
Equity Investor**

Board member

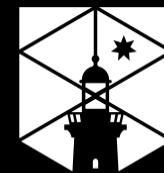
**Exclusive
Commercial IP
Licensing**

**Research
partnership /
collaboration**

Access to HPC infrastructure

**Campus Work
Space and
Admin Support**

**Research
Student
Contributions**



MACQUARIE
University

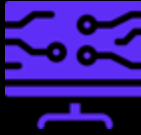
05

Ask

Use of Funds

Seed Investment

Apate.AI is seeking **seed funding** for the commercialisation of the AI-Callee and Insights products



Technology

Product-led development costs associated with the AI-Callee solution and Insights for enterprise and government products.



People

Hiring engineers and product managers to accelerate the development of the core products through the design partner programs



Design Partner Programs

Offset costs for strategic design partners supporting the refinement of product market fit for the telecommunications providers, enterprises and large Government Organisations



Customer Aquisition

Marketing and promotions of Apate.AI to future customers

06

Appendix

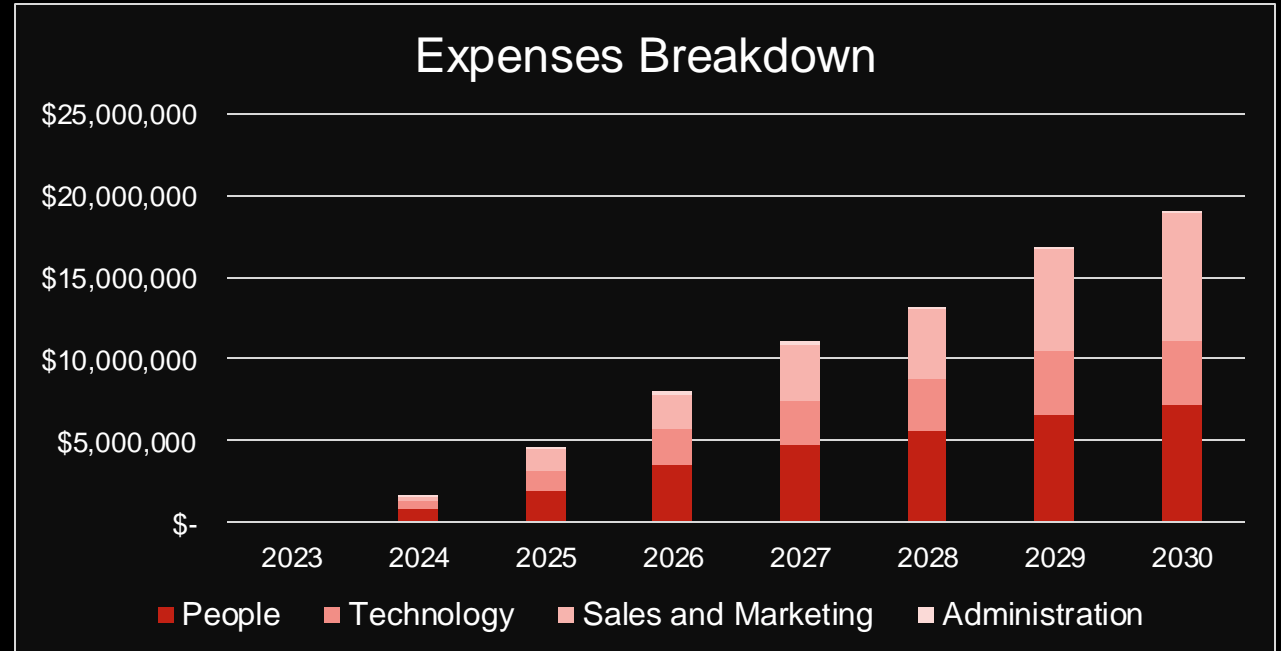
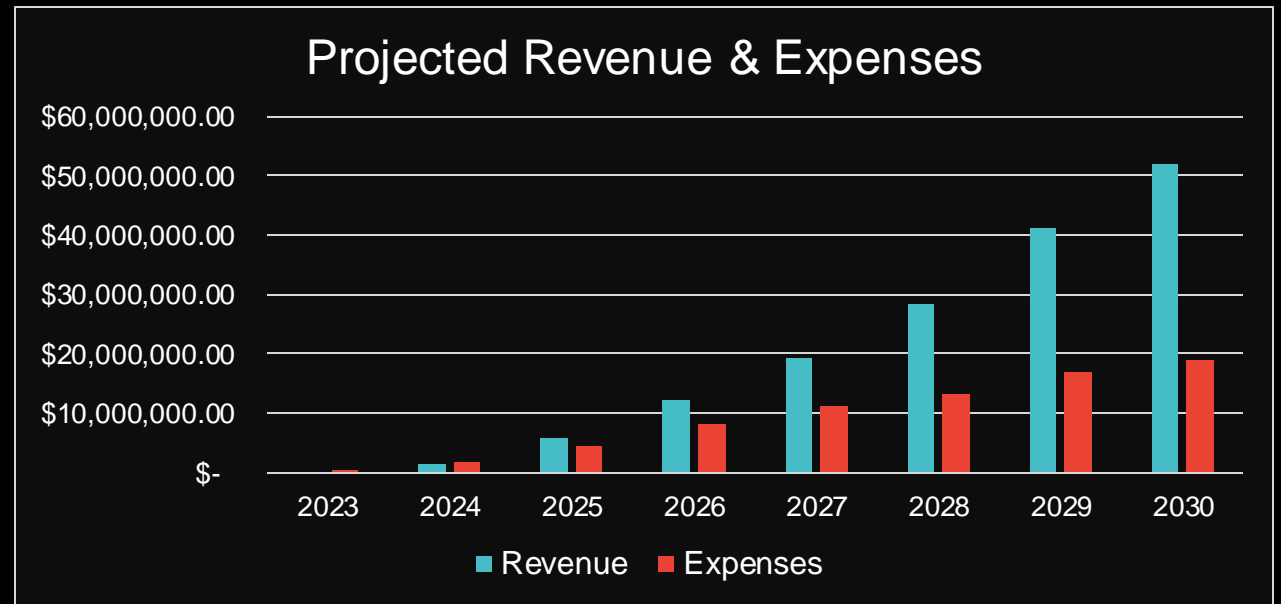
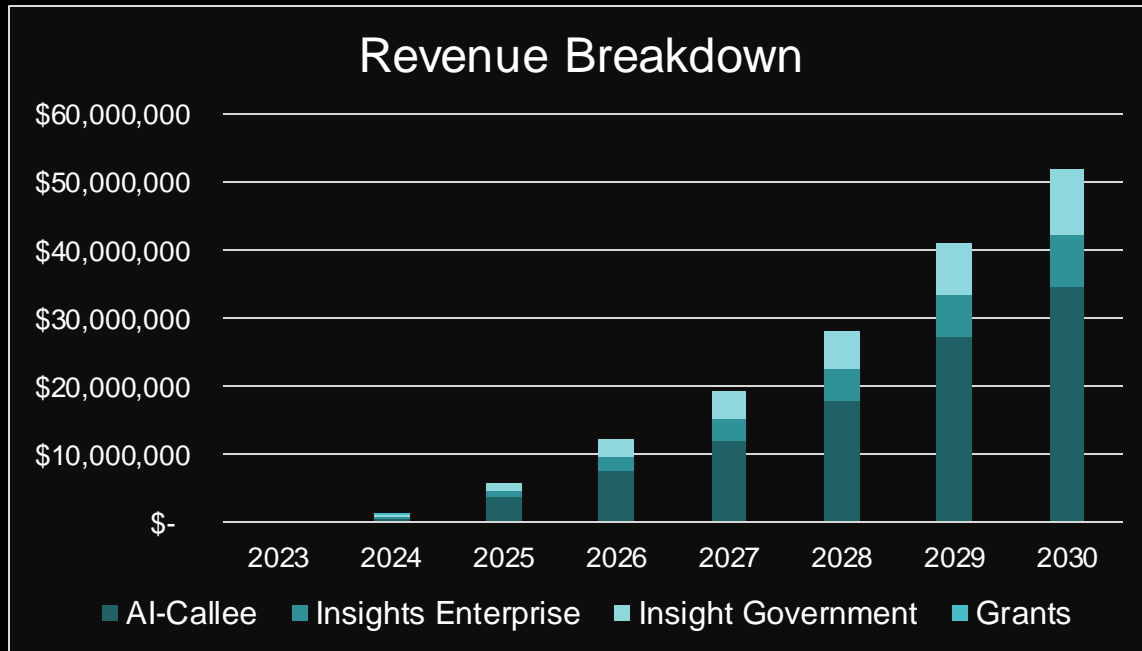
Revenue Model

Financial Forecast

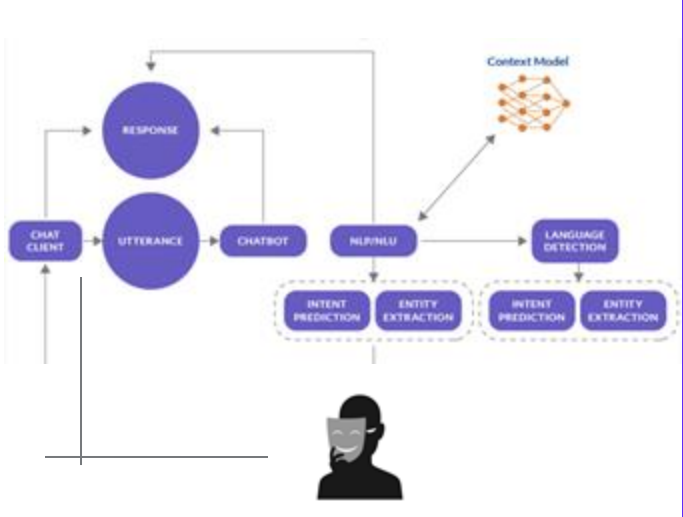
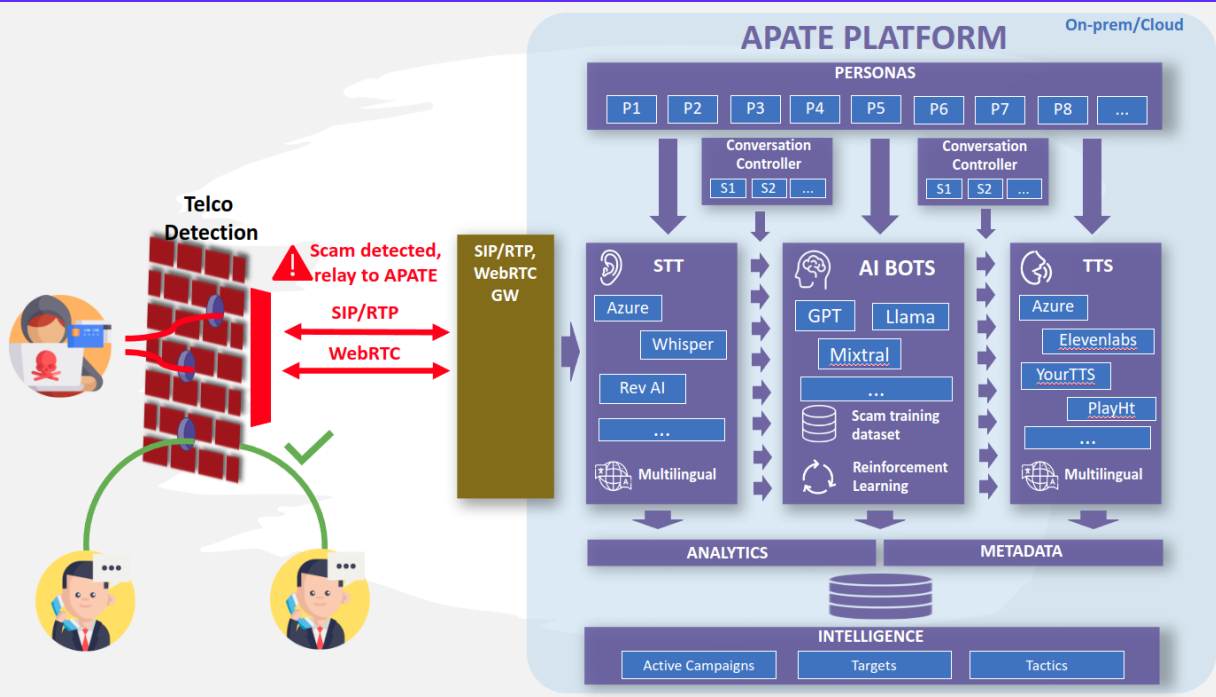
Neutral Case

Projected revenue and expenses 2023-2030

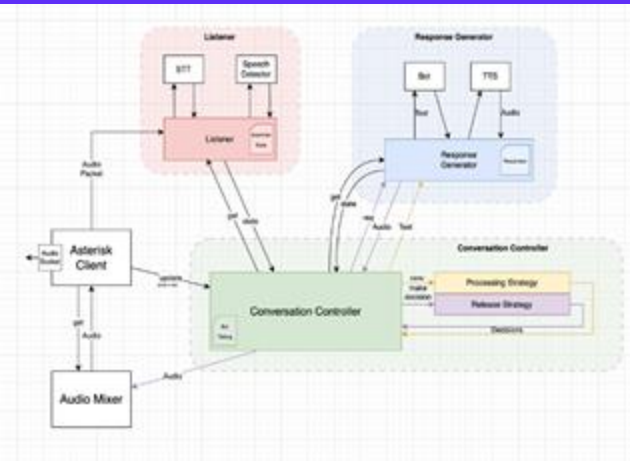
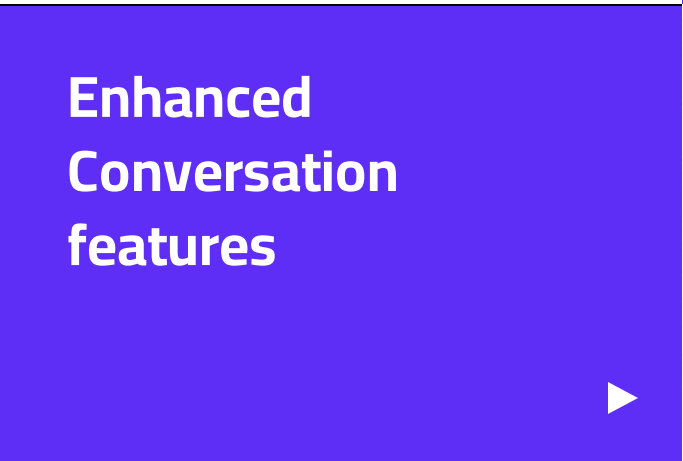
[Link to Financial Forecast](#)



DevOps Pipeline (SIP and WebRTC compliant)



Embedded Shared Mental Models



The Technology

What we have built

Configuration List

Add Config

Doug Mitchell (Guy, Whisper)

Created: 2023-07-21 08:50:30
Modified: 2023-08-29 07:03:05
Uses: 73

Associated Numbers:
61255260572, 61256268069,
61256323099, 61258367092,
61260810093, 61264368015

EditViewDelete

Bernard Stapien (Whisper, Merge Calls)

Created: 2023-07-24 02:42:14
Modified: 2023-09-13 01:51:01
Uses: 13

Associated Numbers:
61480096725

EditViewDelete

Bernard Stapien (Coqui, Whisper Calls)

Created: 2023-07-25 03:12:48
Modified: 2023-09-20 00:59:54
Uses: 525

Associated Numbers:
* (Default), 61291880650

EditViewDelete

Doug Mitchell, Truck Driver (Coqui, Rev)

Created: 2023-08-02 02:13:33
Modified: 2023-08-29 07:11:12
Uses: 8

Associated Numbers:
61283535360, 61863655375

EditViewDelete

Arvind Mehta, Indian Entrepreneur

Created: 2023-08-17 01:11:21
Modified: 2023-08-24 07:39:56
Uses: 22

Associated Numbers:
61242110152, 61260611083, 61280465370,
61287552654, 61288454866

EditViewDelete

Elma Fisher (Coqui, For Examples)

Created: 2023-08-24 07:20:36
Modified: 2023-08-24 07:25:46
Uses: 2

Associated Numbers:
61243131806

EditViewDelete

Bernard Stapien (Coqui, For Examples)

Created: 2023-08-28 23:18:21

Jenny (Chat) with BB

Created: 2023-08-28 23:18:21

Jessica Mitchell (Jenny Chat)

Created: 2023-08-29 07:06:19

▲
Configuration List

Configuration

Back to Config List Edit this Config Delete this Config

Doug Mitchell (Guy, Whisper)

Phone Numbers:
61255260572 61256268069 61256323099 61258367092 61260810093 61264368015

JSON information:

```
{
  "tts": {
    "tts_provider": "AZURE",
    "voice_name": "en-US-GuyNeural",
    "universal_ssl": {}
  },
  "stt": {
    "stt_provider": "WHISPER",
    "speech_detection": {
      "speech_prob_threshold": 0.3,
      "ipw_threshold": 0.2,
      "enable_stt_thresholds": false
    }
  },
  "bot": {
    "bot_server_submitted": "BotGPT",
    "bot_first_messages": [],
    "bot_talk_first": false,
    "silent_convo_seed": [],
    "context": "Act as an American Truck driver from Tulsa, Oklahoma.\n Your name is Doug Mitchell.\n You",
    "min_sentence_words": 1,
    "time_wasting_freq": 0,
    "enable_disfluencies": false,
    "bot_server": "ws://bot-gpt:8002/"
  },
  "audio_mixer": {
    "max_buffer": 40,
    "background_audio": "RANDOM",
    "background_volume": 0.05,
    "bot_volume": 1,
    "effects": "[]"
  }
}
```

Back to Config List Edit this Config Delete this Config

Back to Config List

Phone Number List

Phone Number

Phone Numbers:

Phone Number	Config
61264368015	Doug Mitchell (Guy, Whisper) View Config Edit Config Unlink Config
* (Default)	Bernard Stapien (Coqui, Whisper) View Config Edit Config Unlink Config
61480096725	Bernard Stapien (Whisper, Merge Calls) View Config Edit Config Unlink Config
61291880198	Aussie Edna Fisher (GPT-whisper-azure) View Config Edit Config Unlink Config
61863655375	Doug Mitchell, Truck Driver (Coqui, Rev) View Config Edit Config Unlink Config
61291599113	Jenny (Chat) with BB View Config Edit Config Unlink Config
61242110152	Arvind Mehta, Indian Entrepreneur View Config Edit Config Unlink Config
61243131806	Elma Fisher (Coqui, For Examples) View Config Edit Config Unlink Config
61244807796	Bernard Stapien (Coqui, For Examples) View Config Edit Config Unlink Config
61245479985	Jessica Mitchell (Jenny Chat)

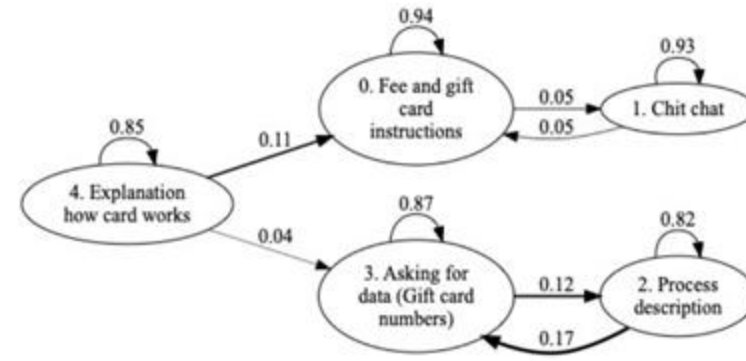
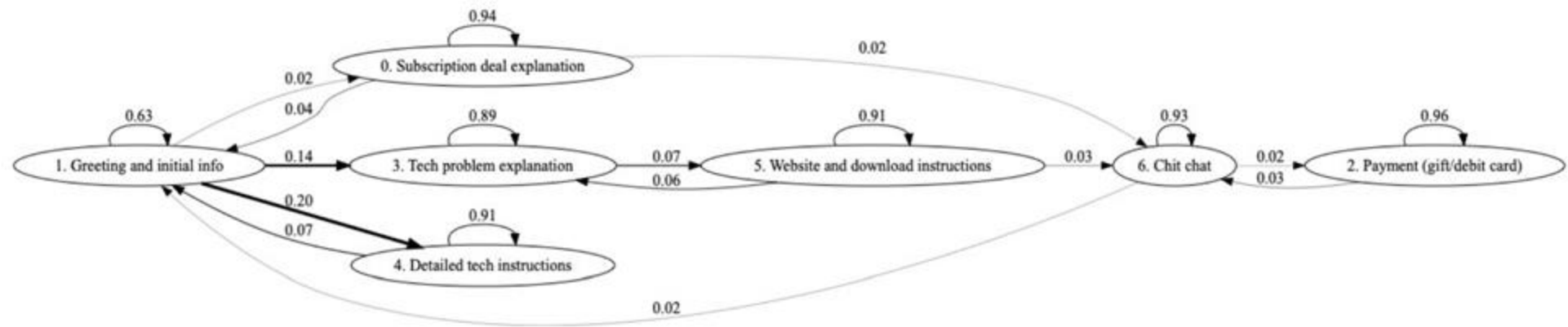
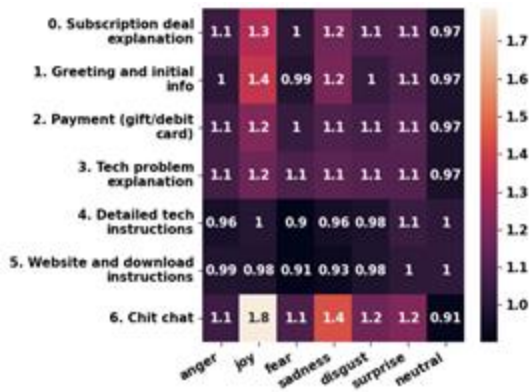
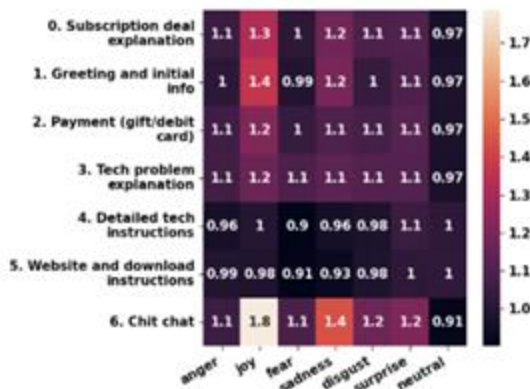
▲
Phone Number List

Apate Personas

06 - Appendix

Context and Scam Category Awareness

Scam Baiters Minded



▲ HMM state transition graph for "Technical Support" scams

◀ HMM state transition graph for "reward" scams

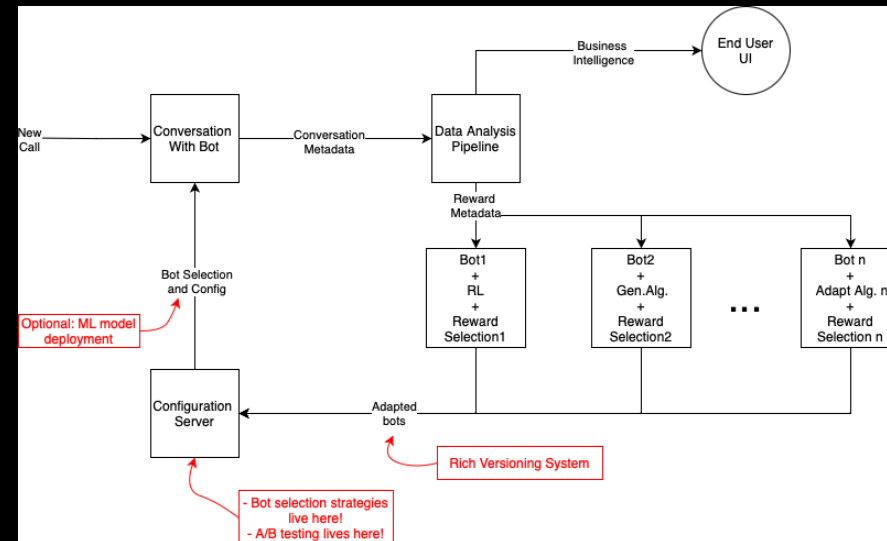
Embedded Shared Mental Models

The Technical Details

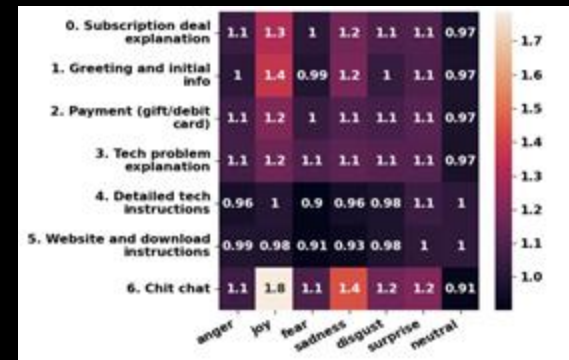
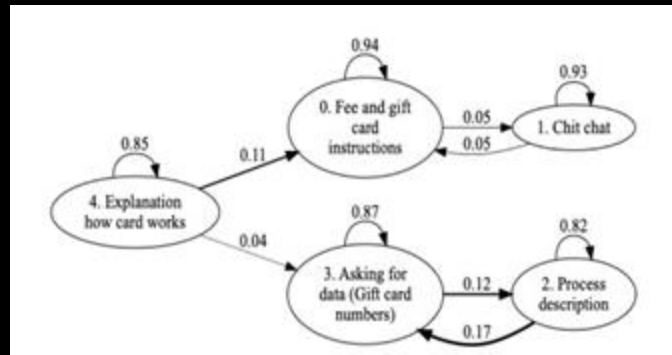
The Apate Bot is optimized for longer conversations.

The **Context Model** is updated based on the success or failure of current strategies - using Reinforcement Learning.

During the conversation, the bot derives the intent of the scammer and reacts in a way to deceive them from reaching advanced stages of their scam script/plot.



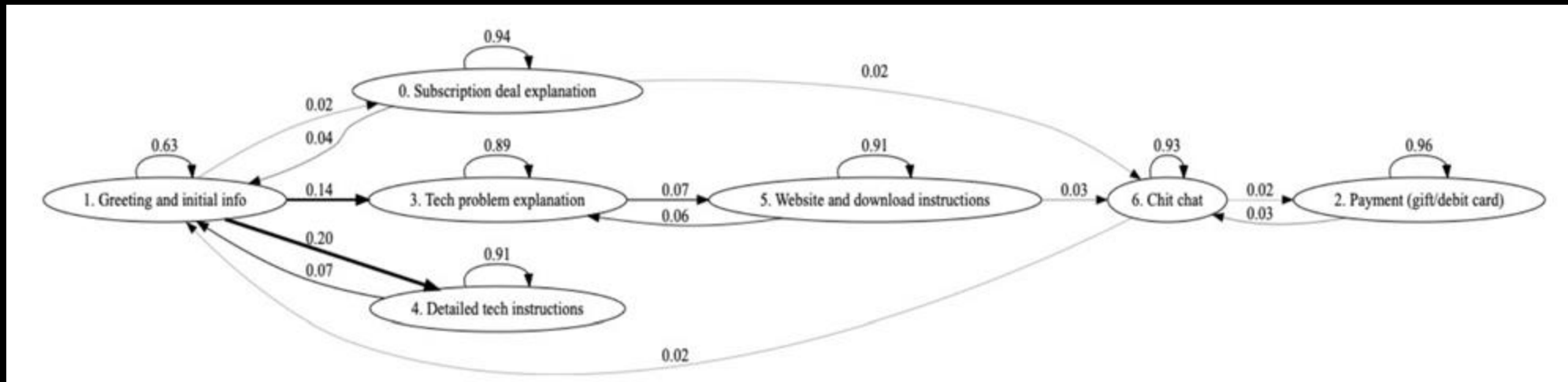
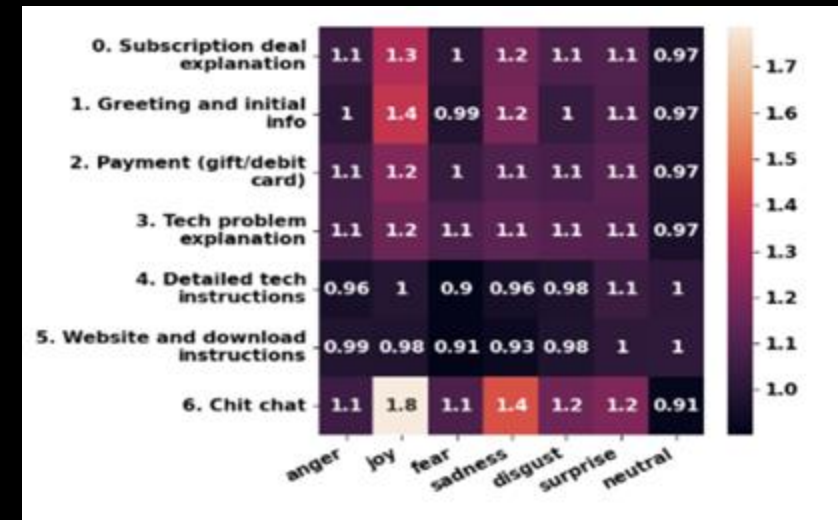
Probabilistic model for Reward Scams



Probabilistic Model for Technical Support Scams

The Technical Details

Hidden Markov Models (HMM) are probabilistic models. These probabilistic models of scams allow us to infer conversation status from observed data. These transition graphs allow us to get inside the head of the scammers to bait them.

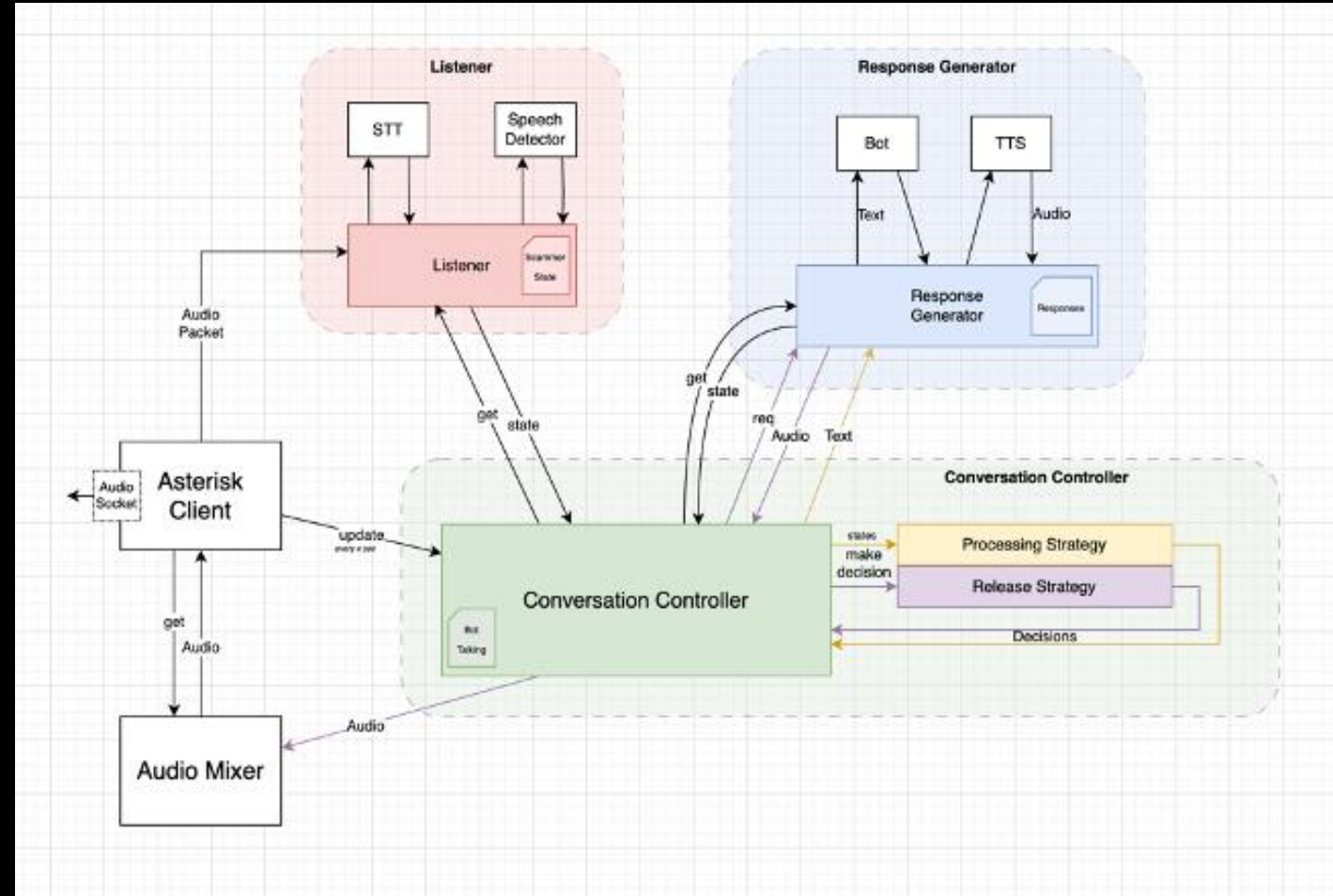


Enhanced Conversation Features

The Technical Details

A **Conversation Controller** manages listening and talking. This includes enhanced conversational features to create a human-like voice, realistic interplay between interlocutors with injection of disfluencies, emotions, backchannelling and minimized speech delays.

The result? A flexible asynchronous conversation control architecture that intelligently manages turn taking and conversation **based on a deep knowledge of scammer/victim conversation structure**.



Flexible & Infinitely Scalable

The Technical Details

On-Prem or Cloud – containerized solution flexibly adapted depending on customer preference and data/intelligence acquisition requirements

Easy to integrate with existing in-house offerings – we can customize voices, bot personas, speech recognition and incorporate a wide-range of existing in-house LLMs and trained AI models.

DevOps Pipeline - SIP and WebRTC compliant

