sardine

Emerging Fraud and Scam Typologies

Presented by:

Soups Ranjan

CEO and co-founder

Soups Ranjan

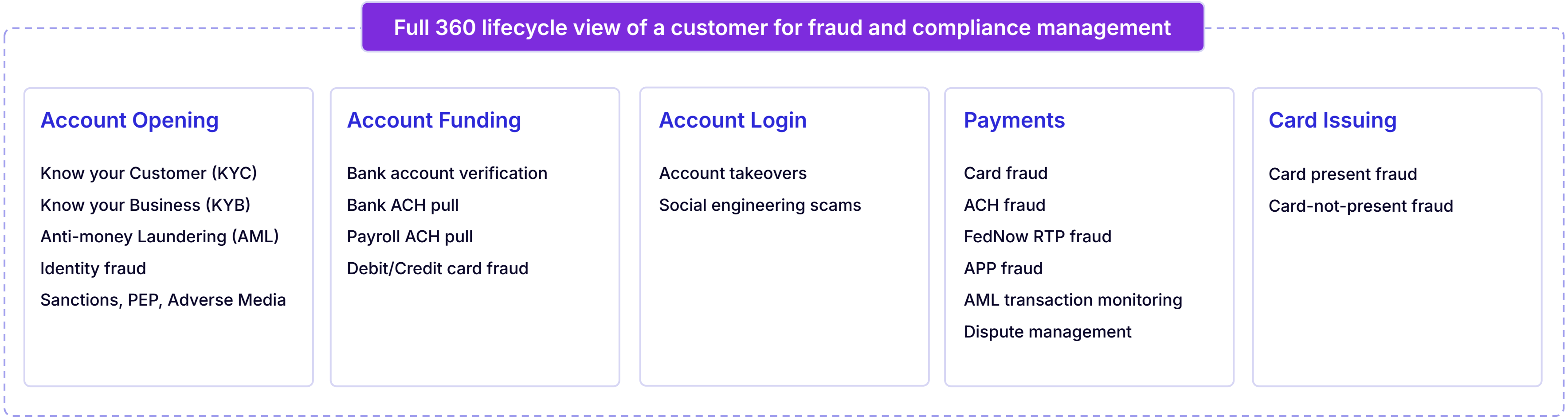
Co-founder and CEO, Sardine

A bit about me:

- **15+ years using ML to fight financial crime**
- **Led Risk & Data science teams, built high-performance fraud and compliance stacks**
  - Scaled Coinbase by 1000x
  - Launched Revolut US
- **Passionate about sharing knowledge w the risk community!**
  - Founded Risk Salon community
  - Now we host Fraud Squad events

Continuous monitoring across all customer touchpoints

To create a risk platform that works really well, you often have to stitch together 30+ vendors, each of which are point-solutions and monitor only one aspect of customer lifecycle. With Sardine, you can monitor the customer lifecycle end-to-end with one solution.



Full 360 lifecycle view of a customer for fraud and compliance management

Account Opening

- Know your Customer (KYC)
- Know your Business (KYB)
- Anti-money Laundering (AML)
- Identity fraud
- Sanctions, PEP, Adverse Media

Account Funding

- Bank account verification
- Bank ACH pull
- Payroll ACH pull
- Debit/Credit card fraud

Account Login

- Account takeovers
- Social engineering scams

Payments

- Card fraud
- ACH fraud
- FedNow RTP fraud
- APP fraud
- AML transaction monitoring
- Dispute management

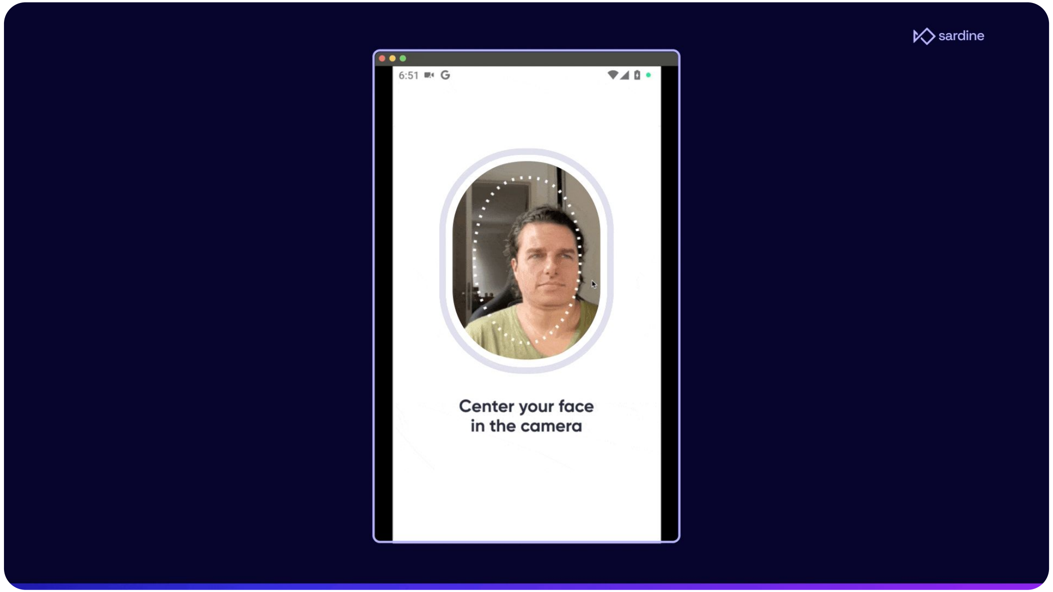
Card Issuing

- Card present fraud
- Card-not-present fraud

sardine

Does the rise in deep fakes mean that *ID proofing is dead*?

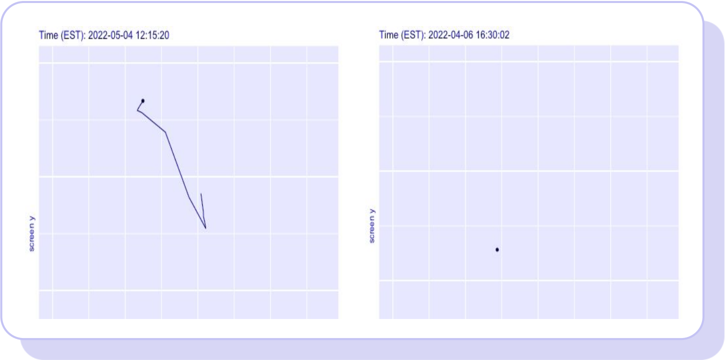
Extrinsic AI vs Intrinsic AI: The future of online identity is a battle of bots



Catch fraudsters by their intrinsic behavior, because everyone has a *tell*...

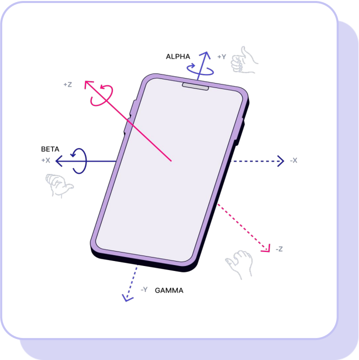
Expert fraudster detection

Normal customers cover a large surface area with their mouse, while fraudster mouse patterns exhibit expert knowledge of a website.



Phone theft detection

We can predict **bank account** logins from a stolen phone with **85% accuracy**.



Bot detection

Humans can't type on their phones while they are face down on table.

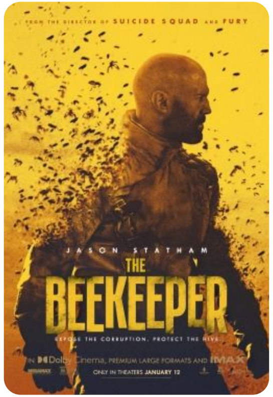
Anatomy of a scam

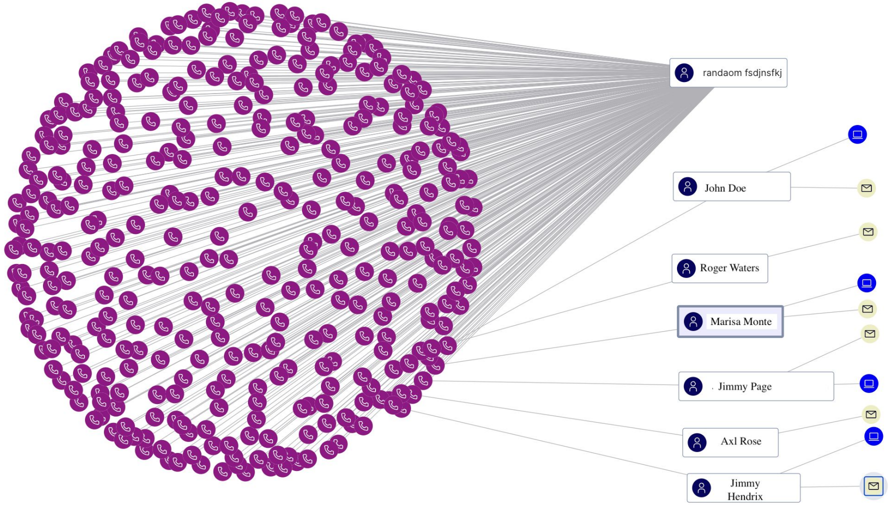
Bank impersonation scams: How do fraudsters find victims?

👉 Fraudsters try a series of phone numbers during the onboarding flow of a bank

👉 When the bank says “Welcome back, name!” They know they have a hit

👉 Then they use this information to run a scam against the user by pretending to be the bank

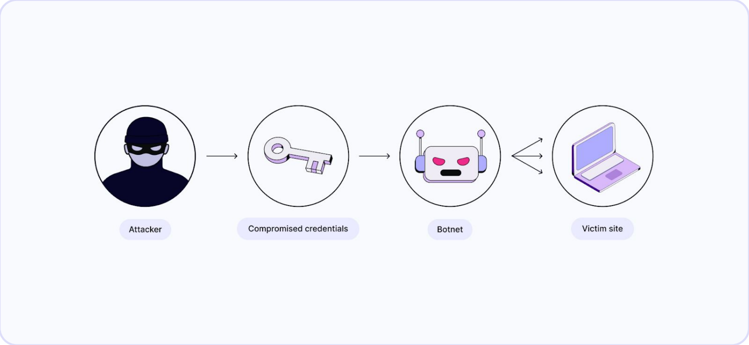

FROM THE DIRECTOR OF SUICIDE SQUAD AND FURY
JASON STATHAM
THE BEEKEEPER
EXPOSE THE CORRUPTION. PROTECT THE HIVE.
ONLY IN THEATERS JANUARY 12

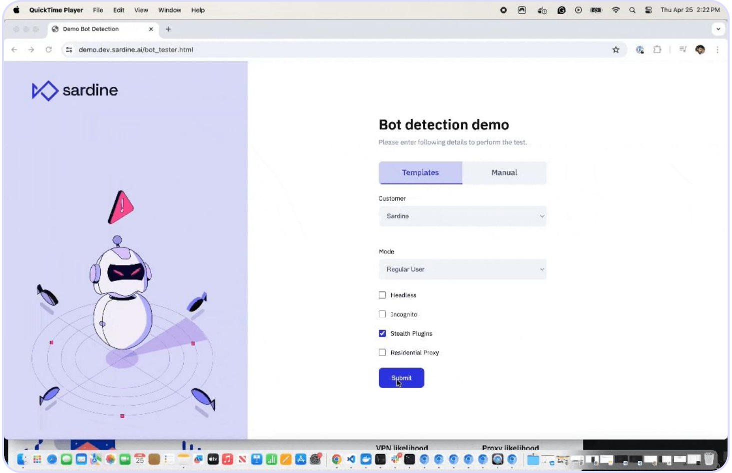


Bank impersonation scams: Google ad followed by replay of credentials using a bot

👉 Fraudster next creates a lookalike site to the bank

👉 When the victim logs in to the lookalike site, they replay the credentials in real-time using a script or a bot





Bot detection demo

Please enter following details to perform the test.

Templates | Manual

Customer: Sardine

Mode: Regular User

☐ Headless

☐ Incognito

☑ Stealth Plugins

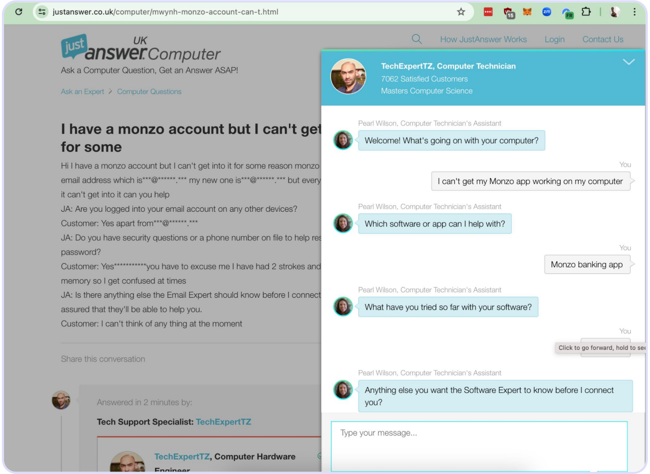
☐ Residential Proxy

Submit

Bank impersonation scams: Fraudster advertises a fake bank support phone number

👉 Fraudster may not even need to create a lookalike site

👉 They just advertise “bank support phone number” and then use TeamViewer to control victim’s screen



justanswer.co.uk/computer/mwynh-monzo-account-can-t.html

Ask a Computer Question, Get an Answer ASAP!

Ask an Expert > Computer Questions

I have a monzo account but I can't get
for some

Hi I have a monzo account but I can't get into it for some reason monzo
email address which is***@******.*** my new one is***@******.*** but every
it can't get into it can you help

JA: Are you logged into your email account on any other devices?

Customer: Yes apart from***@******.***

JA: Do you have security questions or a phone number on file to help res
password?

Customer: Yes***********you have to excuse me I have had 2 strokes and
memory so I get confused at times

JA: Is there anything else the Email Expert should know before I connect
assured that they'll be able to help you.

Customer: I can't think of any thing at the moment

Share this conversation

Answered in 2 minutes by:

Tech Support Specialist: TechExpertTZ

TechExpertTZ, Computer Hardware Engineer

TechExpertTZ, Computer Technician
7062 Satisfied Customers
Masters Computer Science

Pearl Wilson, Computer Technician's Assistant
Welcome! What's going on with your computer?

You
I can't get my Monzo app working on my computer

Pearl Wilson, Computer Technician's Assistant
Which software or app can I help with?

You
Monzo banking app

Pearl Wilson, Computer Technician's Assistant
What have you tried so far with your software?

You

Pearl Wilson, Computer Technician's Assistant
Anything else you want the Software Expert to know before I connect you?

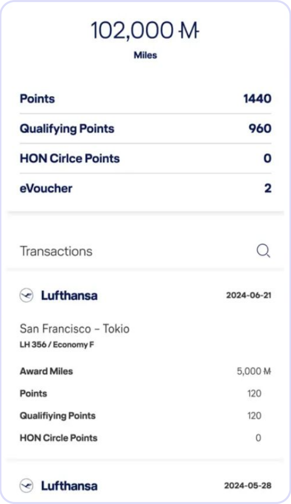
Type your message...

sardine

If it looks like a bank...
talks like a bank...
smells like a bank...

...to a fraudster, it’s a bank

Account Takeover: A fraudster takes control of your loyalty points account and redeems the points for cash



102,000 M

Miles

Points	1440
Qualifying Points	960
HON Cirlce Points	0
eVoucher	2

Transactions

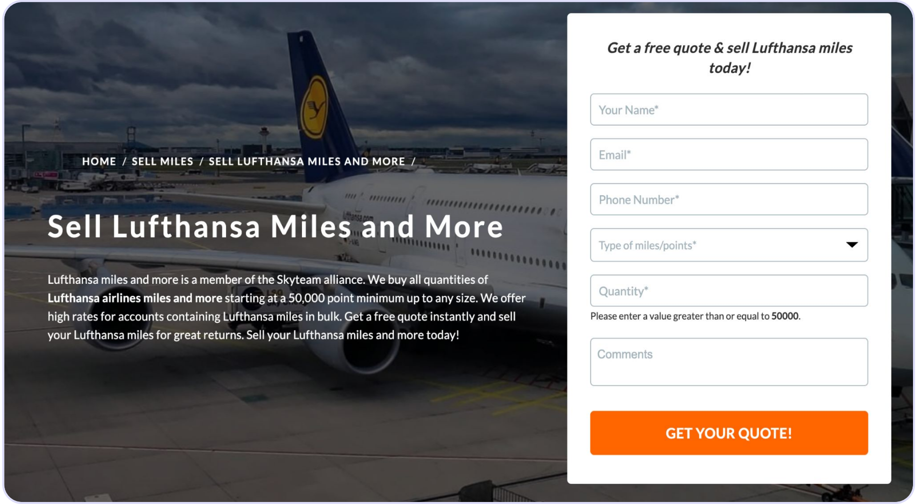
Lufthansa 2024-06-21

San Francisco – Tokio

LH 356 / Economy F

Award Miles	5,000 M
Points	120
Qualifiying Points	120
HON Circle Points	0

Lufthansa 2024-05-28



HOME / SELL MILES / SELL LUFTHANSA MILES AND MORE /

Sell Lufthansa Miles and More

Lufthansa miles and more is a member of the Skyteam alliance. We buy all quantities of **Lufthansa airlines miles and more** starting at a 50,000 point minimum up to any size. We offer high rates for accounts containing Lufthansa miles in bulk. Get a free quote instantly and sell your Lufthansa miles for great returns. Sell your Lufthansa miles and more today!

Get a free quote & sell Lufthansa miles today!

Your Name*

Email*

Phone Number*

Type of miles/points* ▼

Quantity*

Please enter a value greater than or equal to **50000**.

Comments

GET YOUR QUOTE!

sardine

Wherever there's money movement

There are scams

Every online payment has a potential scam lurking

Common scams

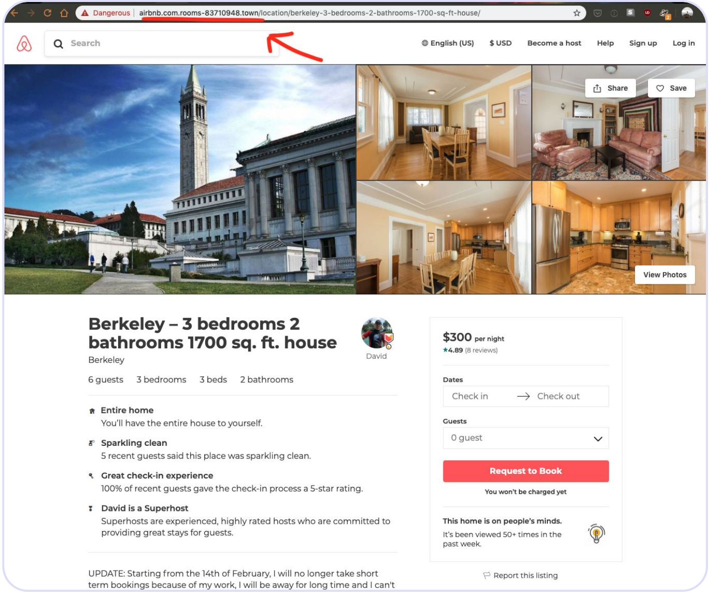
- Romance scams
- Investment advisor
- Business email compromise (BEC)
- Fake tech support
- Phishing scams
- Fake giveaways

Emerging scams

- Rent payment scams
- Hotel booking scams
- Air travel booking scams
- Fake seller scams
- Uber driver scams
- QR code scams

Next time you make a rent payment online, don’t search for its site online. Go directly to the property manager’s website

- These websites look identical to the real thing. See that airbnb logo? Looks legit.
- But take a closer look at that domain http://airbnb.com.rooms-83710948.town
- That’s right, it’s a phishing site.



Dangerous | airbnb.com.rooms-83710948.town/location/berkeley-3-bedrooms-2-bathrooms-1700-sq-ft-house/

Berkeley – 3 bedrooms 2 bathrooms 1700 sq. ft. house

Berkeley

David

6 guests 3 bedrooms 3 beds 2 bathrooms

Entire home
You’ll have the entire house to yourself.

Sparkling clean
5 recent guests said this place was sparkling clean.

Great check-in experience
100% of recent guests gave the check-in process a 5-star rating.

David is a Superhost
Superhosts are experienced, highly rated hosts who are committed to providing great stays for guests.

UPDATE: Starting from the 14th of February, I will no longer take short term bookings because of my work, I will be away for long time and I can't

$300 per night
★4.89 (8 reviews)

Dates: Check in → Check out

Guests: 0 guest

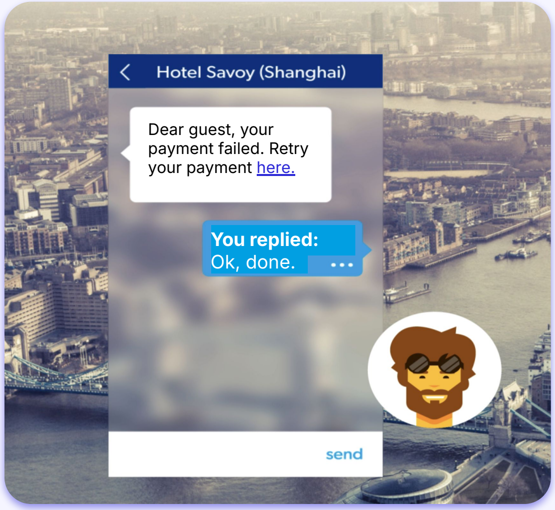
Request to Book

You won’t be charged yet

This home is on people’s minds.
It’s been viewed 50+ times in the past week.

Report this listing

Scammers socially engineer hotel employees to change payout links for guests



Dear guest, your payment failed. Retry your payment here.

You replied: Ok, done.

How can you detect this?

Prevent this at the weakest link – hotel employee getting scammed

Sardine's Remote Access Tool (RAT) detection can identify if an employee was guided with a screen sharing tool like TeamViewer.

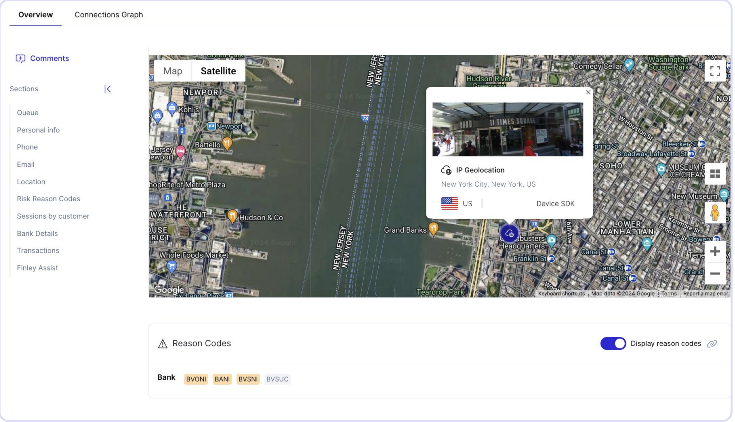
Scammer tricks you into buying an airline ticket with a fake fuel surcharge

- Criminals create a site that looks like a real travel agency.
- User hits the fake site and thinks they've booked a trip
- Criminal then creates a transaction for a real flight PLUS a fake fuel surcharge.

How can you detect this?

Fraudster is likely creating a transaction on real site while masking their IP

Sardine's True Piercing™ technology pierces through the VPN/proxy to identify fraudster's True IP and True Location

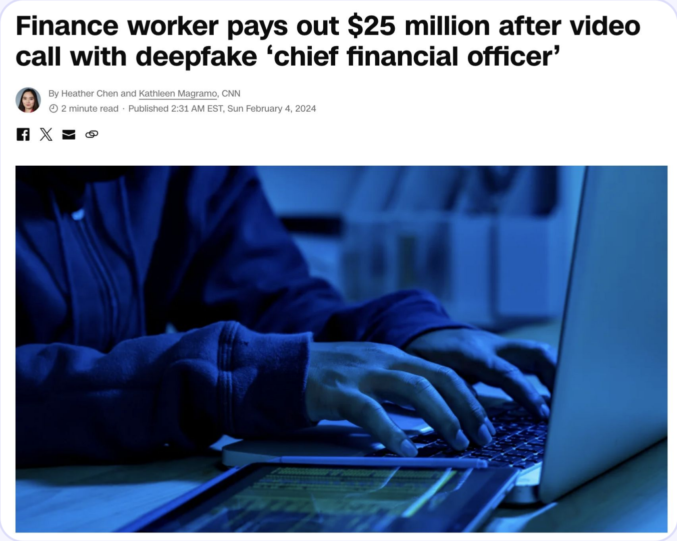


IP Geolocation
New York City, New York, US
US | Device SDK

Reason Codes

Bank BVONI BANI BVSNI BVSUC

Deepfakes are making Business Email Compromise infinitely scalable



Finance worker pays out $25 million after video call with deepfake ‘chief financial officer’

By Heather Chen and Kathleen Magramo, CNN
2 minute read · Published 2:31 AM EST, Sun February 4, 2024

How can you detect this?

The key is to monitor the full customer lifecycle from login to payments.

Sardine collects device data at the time of login – to see if payee bank details are changed from a “risky login”. We can then tie this risky login behavior to the payment being made to a brand new IBAN.

Triangulation fraud: Fake sellers intercept purchases and steal your card details

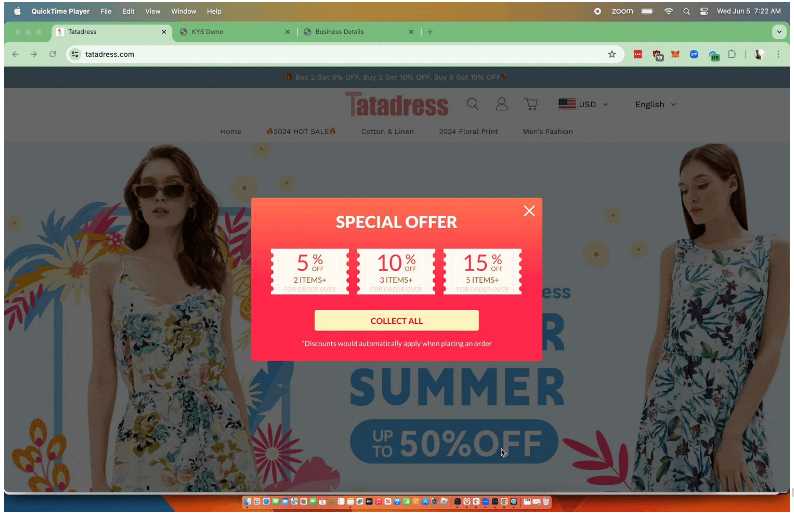
- **Fraudsters advertises a product**, such as shoes on a Nike look-alike website
- **Consumer buys the shoes**
- **Fraudster then buys it** from the actual Nike site and then ships it.
- Fraudster has now **harvested your card details** that they can use elsewhere

How can you detect this?

Merchant risk scoring and KYB.

Sardine helps PayFacs safely onboard merchants by providing them with rich insights into:

- Merchants actual MCC and NAICS codes
- Whether merchant actually ships goods
- Merchant tags for SKUs
- Card transaction volumes



Buy 2 Get 5% OFF, Buy 3 Get 10% OFF, Buy 5 Get 15% OFF

*Discounts would automatically apply when placing an order

Best practices for scam detection

sardine

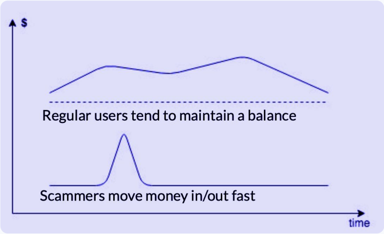
All fraud problems are data science problems

What banks need to combat these threats:

- Lots of data, in high quality
- Trained machine learned models
- Humans in the loop for QA
- That know what to look for!

Which means you need:

- Tools that can capture device and behavior data
- Third-party integrations that enrich your sessions
- ML-based risk scoring with non-generic models
- Centralized dashboard for investigations and case review



Email
Age
Social profile

Phone
Tenure
Line Type

KYC
Synthetic ID
Stolen ID

IP address
Location
Reputation

Bank
Account ID
Blacklisted

Document
Selfie
Liveness check

Chargeback
NSF
Unauthorized

AML
Fiat
Crypto

Sanctions
OFAC
PEP/SDN

Behavior Biometrics

Typing and mouse patterns
Mobile tap and touch
Scrolling patterns
Copy/Paste & Autofill
Hesitation & Distraction
Context switching
Long-term memory recall
Same user vs. Expert

Device Intelligence

Mobile emulator farms
Remote Desktop/TrueOS
Zero-day Proxy/VPN
Network Traffic
Browser fingerprint
Device ID
Accelerometer
Gyroscope

Holistic 360° view of a customer through your bank or app

- **Continuously monitor all sessions** to learn the user's device and behavior patterns, and build a holistic customer profile
- **Patented True Piercing™ technology** unmasks fraudsters hiding behind obfuscated devices
- **Combine device, behavior, identity, and banking data** into one solution to provide a comprehensive view of risk

Full 360 lifecycle view of a customer for fraud and compliance management

Account Opening

Know your Customer (KYC)
Know your Business (KYB)
Anti-money Laundering (AML)
Identity fraud
Sanctions, PEP, Adverse Media

Account Funding

Bank account verification
Bank ACH pull
Payroll ACH pull
Debit/Credit card fraud

Account Login

Account takeovers
Social engineering scams
Payroll ACH pull
Debit/Credit card fraud

Payments

Card fraud
ACH fraud
FedNow RTP fraud
APP fraud
AML transaction monitoring
Dispute management

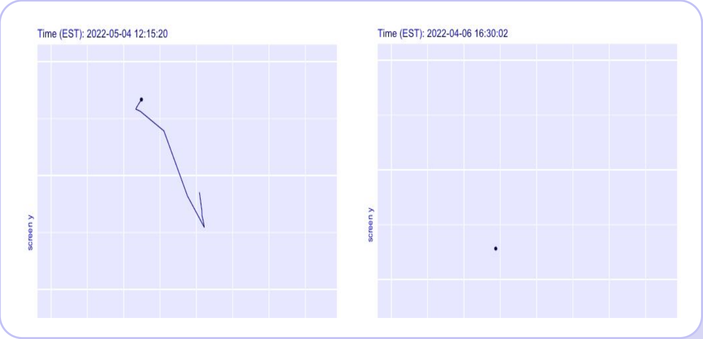
Card Issuing

Card present fraud
Card-not-present fraud

Catch fraudsters by their **intrinsic behavior**, because everyone has a *tell*...

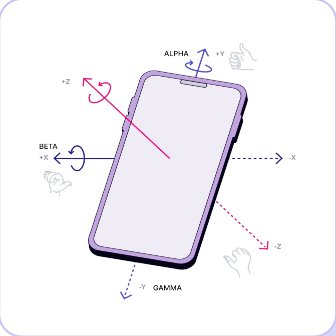
Expert fraudster detection

Normal customers cover a large surface area with their mouse, while fraudster mouse patterns exhibit expert knowledge of a website.



Phone theft detection

We can predict **bank account** logins from a stolen phone with **85% accuracy**.



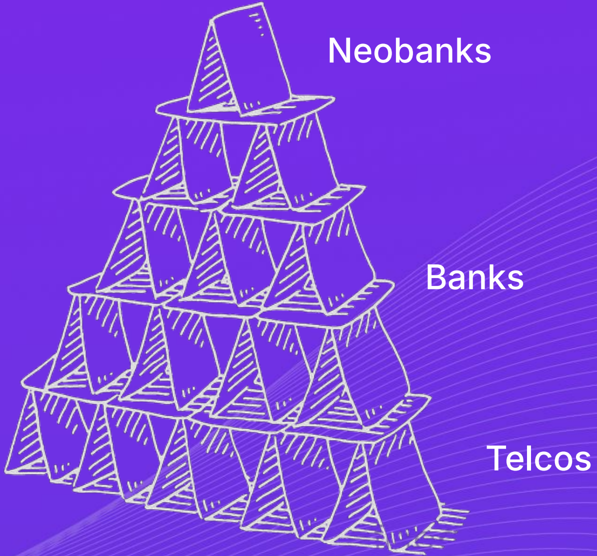
Bot detection

Humans can’t type on their phones while they are face down on table.

Some more observations...

sardine

To solve all fraud and scams, **we might just need a new internet**



We can't trust if the phone call from your bank wasn't spoofed, or DNS cache wasn't poisoned, or the BGP route to the bank wasn't rerouted.

Now add GenAI to it 🤯

sardine

We may also need to enlist the help of social media

One study in the UK said nearly 70% of all APP scams originated on social media

Sonar

Some of these fraud and scam patterns can only be stopped by sharing data across banks, fintechs, social media, telcos

Sonar is an independent, member-run data consortium for sharing real-time insights into First-Party and Counterparty Risk.

Square airbase VISA novo Blockchain.com pipe

ALLOY LABS iLEX CONSULTING GROUP sardine CHESAPEAKE BANK Spring straddle

Thank you.

Contact us for more information:

Soups Ranjan, CEO & co-founder
soups@sardine.ai

www.sardine.ai/contact