Qivox

THE QIVOX SOLUTION

Guy Cooper

Founder

Voice Is Not Enough

Out of Band Multi-layered authentication and device authentication

Focus: Financial Services

SECURITY

- Online and telephone banking requires **authenticating** the user
- Phishing, malware, keyloggers capture user logon details and make a single band authentication too easy to hack

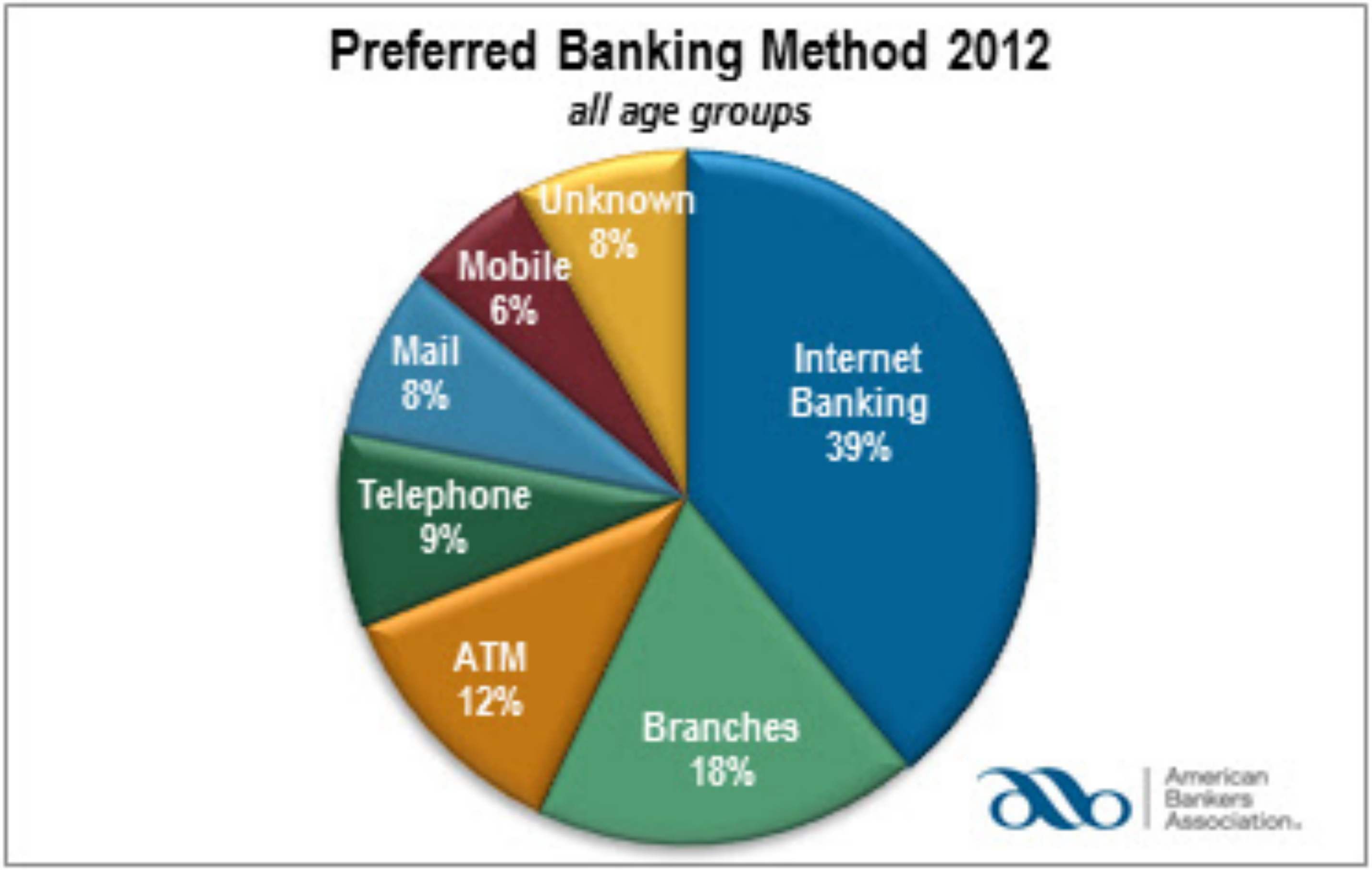
Single-channel voice authentication

- Easy to target – easy to break

A – Fail the test
VB Kryptonite: Noisy environments

B – Social Engineering
Particularly on pre-screen IVR authentication

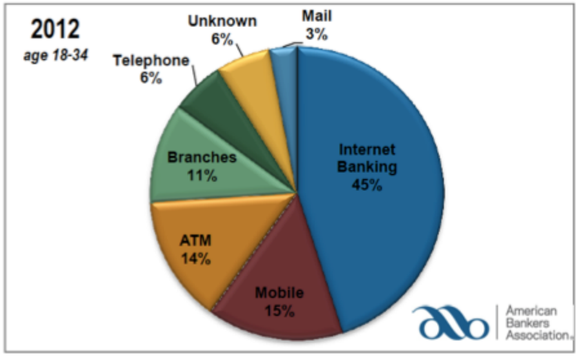
C – Use voice recordings
Pretty good success rate over the phone channel

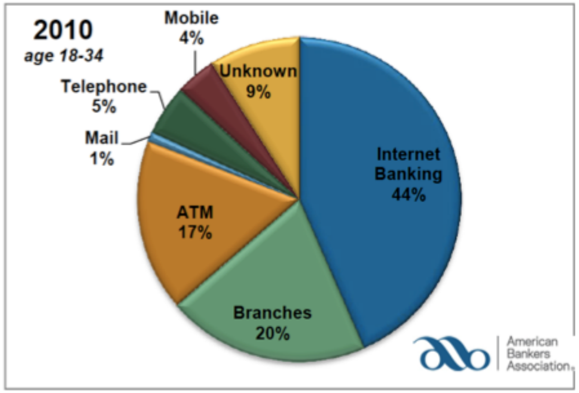

Preferred Banking Method 2012
all age groups
Unknown 8%
Mobile 6%
Mail 8%
Telephone 9%
ATM 12%
Branches 18%
Internet Banking 39%
American Bankers Association

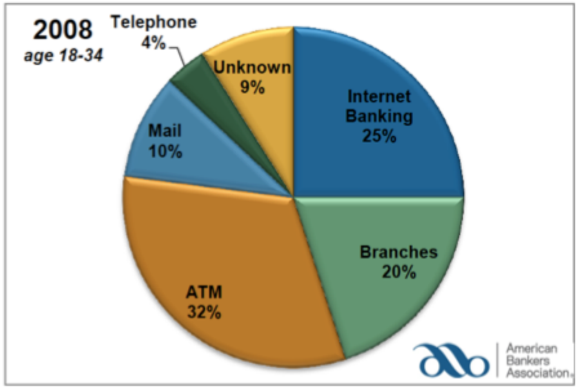
Qivox

Preferred banking Method

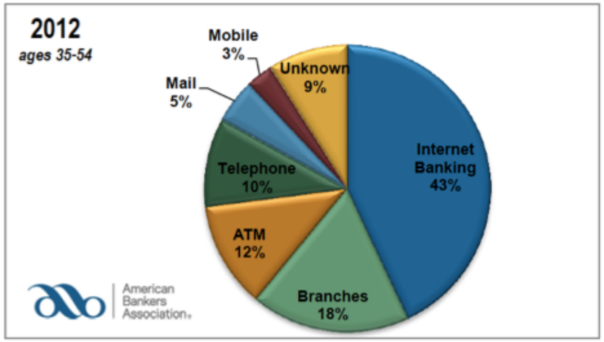
ages 18-34

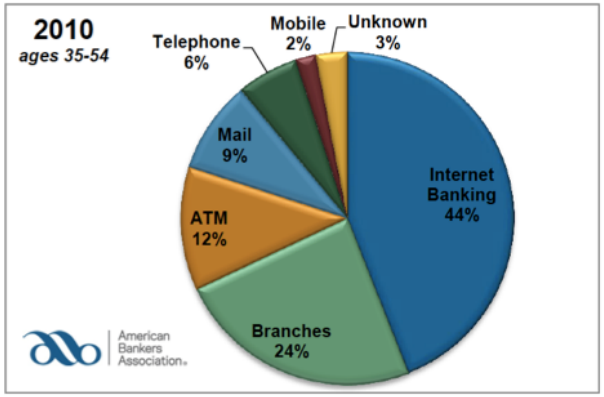


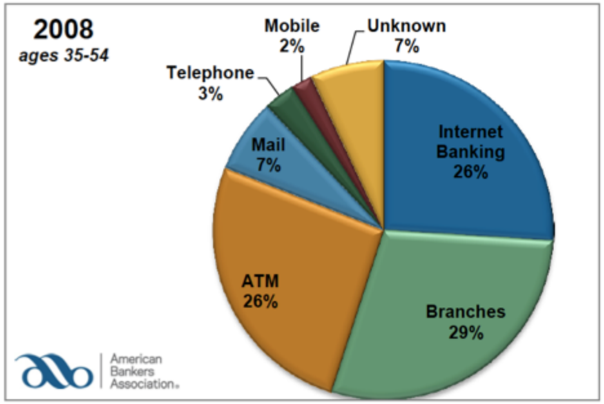




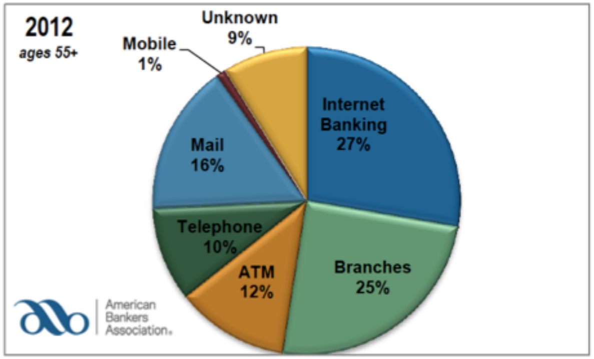
ages 35-54

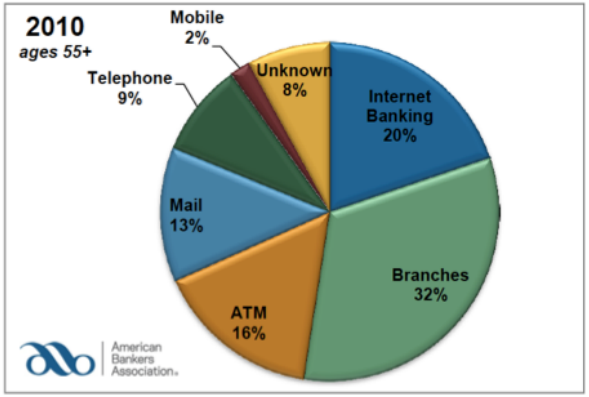


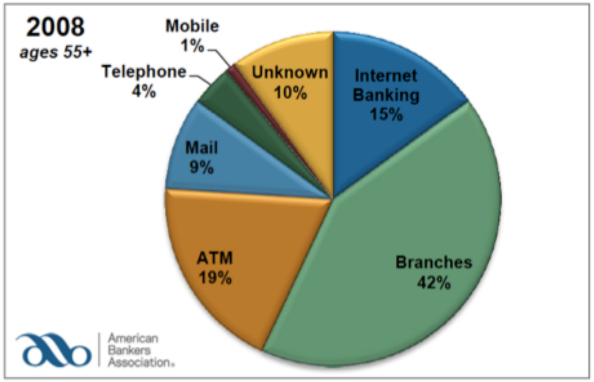


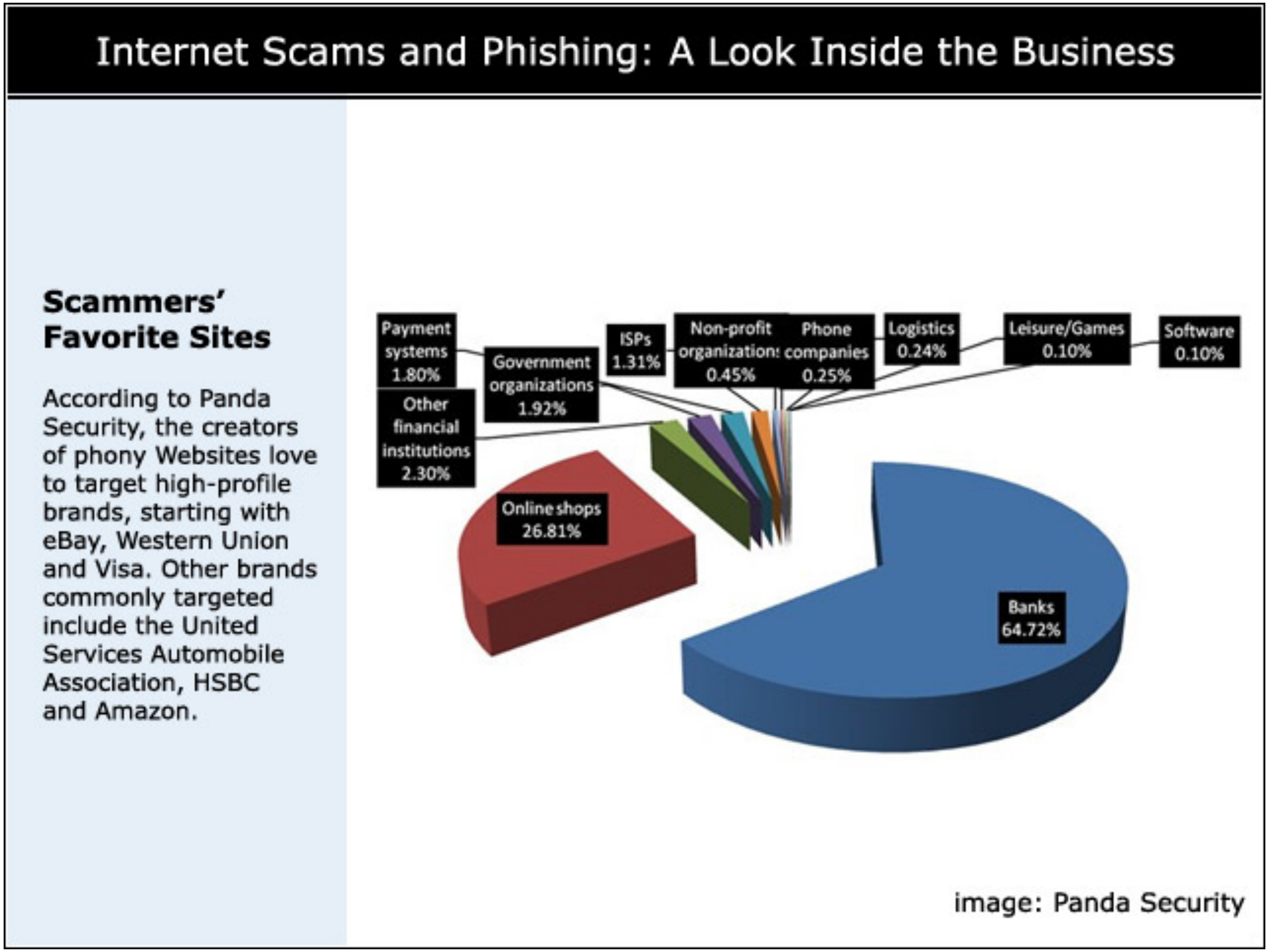


age 55+







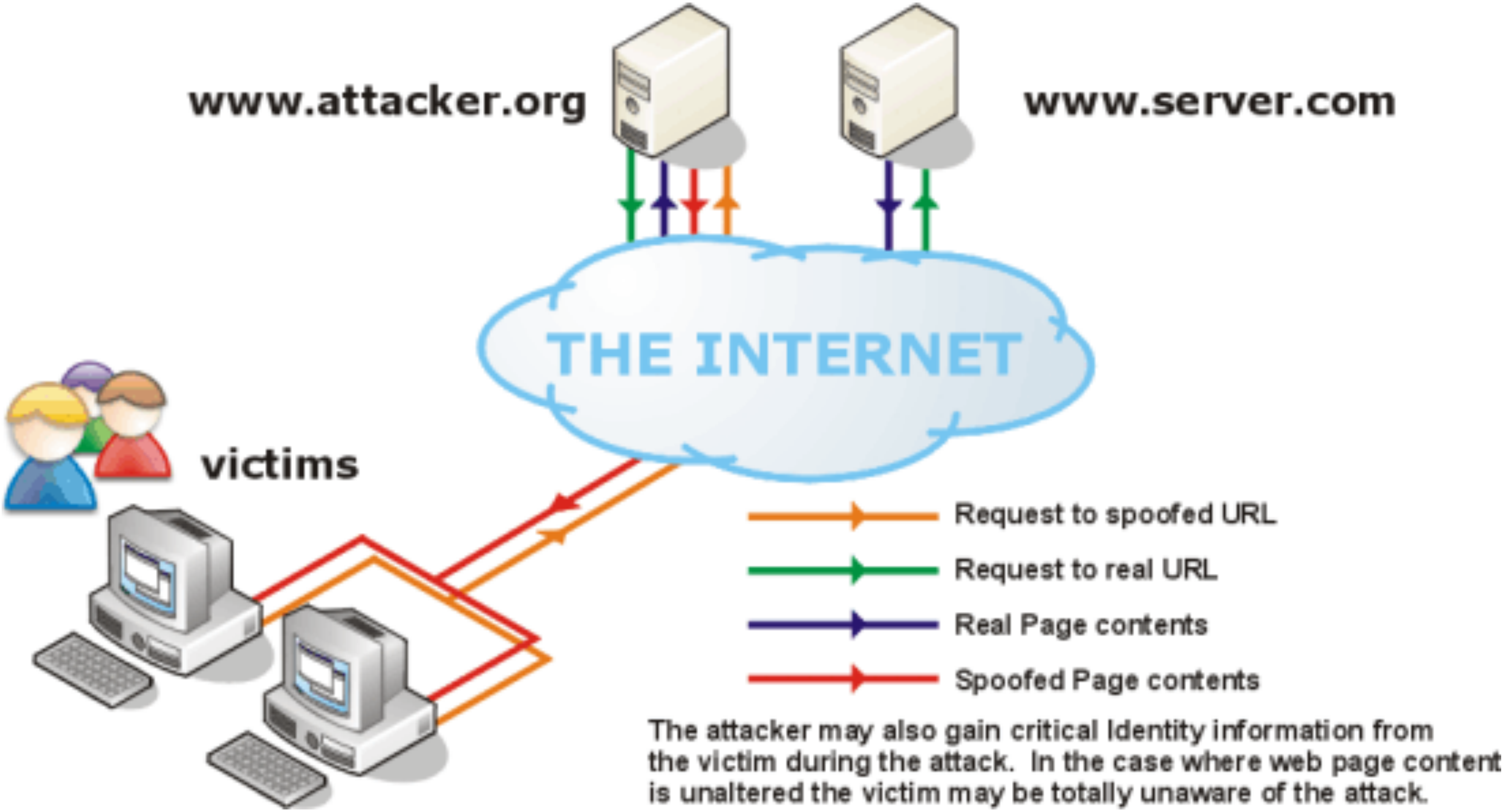


Internet Scams and Phishing: A Look Inside the Business

Scammers' Favorite Sites

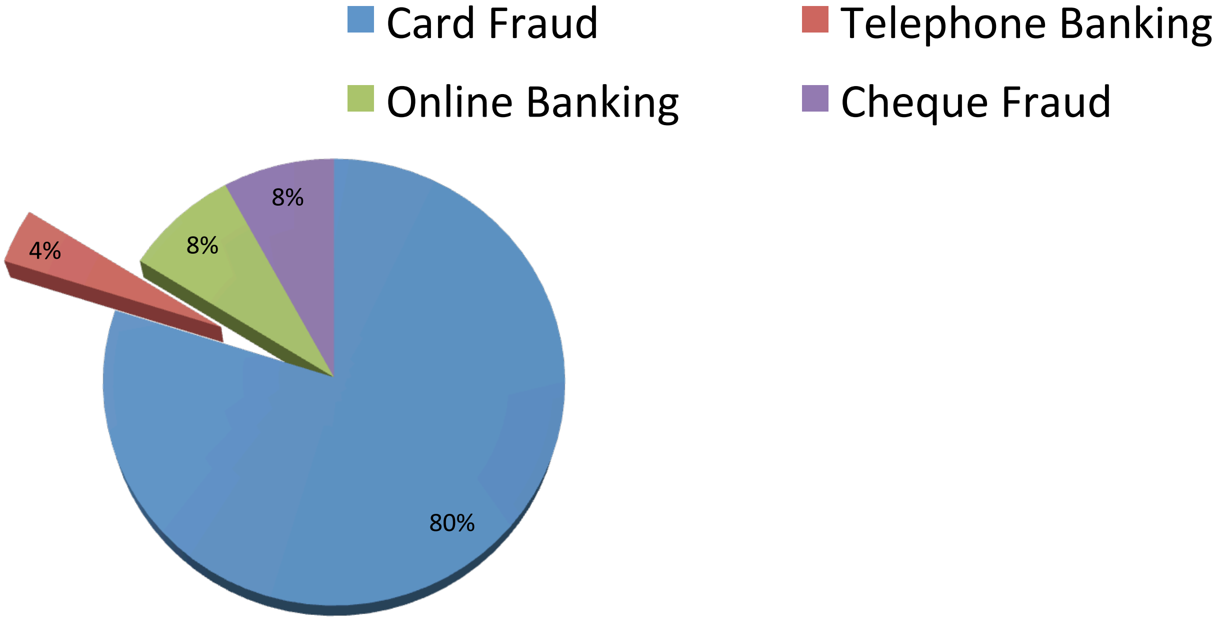
According to Panda Security, the creators of phony Websites love to target high-profile brands, starting with eBay, Western Union and Visa. Other brands commonly targeted include the United Services Automobile Association, HSBC and Amazon.

image: Panda Security



The attacker may also gain critical Identity information from the victim during the attack. In the case where web page content is unaltered the victim may be totally unaware of the attack.

Banking Fraud by Type 2012



The future for Voice Biometrics in Banking?

- First line authentication of the person?

  Customer experience
  Reliability in random circumstances
  Cost per transaction

- First line authentication of the device?

  Banks unlikely to accept self-declared device authentication

- A secondary layer in multi-factor authentication

Anti-Fraud Methods
Out of Band Authentication

- **PIN Sentry**

- **Phone Authentication**

Anti-Fraud Solutions in Financial Services

- One Time PIN
- SIM SWAP
- Mobile and Landline redirect

and layered security

Example use cases

- Password Reset
- PIN view
- Initial Enrolment
- Third party payee set up
- Balance transfer
- Card transaction proximity verification

Security Issues for mobile devices

- Is the call coming from a recognised number

  (CLI spoofing)
- Is the device known?
- Is the location consistent with where I would expect?
- Has anything unusual happened to the device recently?

  Eg phone takeover by SIM Swap
- Is the device on divert to another phone?
- Can I trust my trusted telephone number?
- Is there any other on device authentication?

  Eg token in an App?

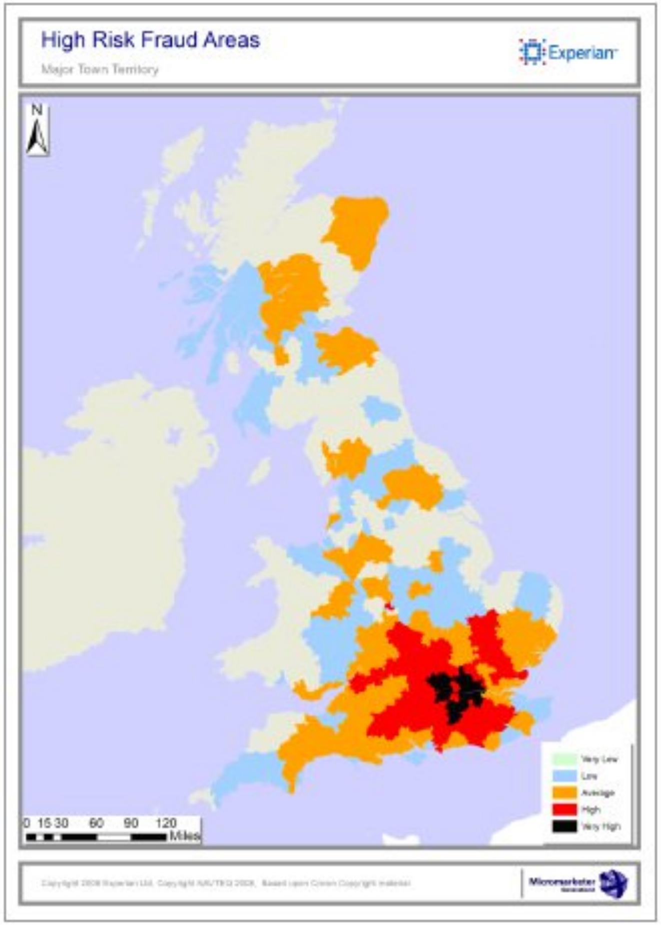
Check Unobtrusively

- SIM SWAP check, library and history
- Redirected numbers
- Geographic location
- Previous Fraud History
- External data comparisons – IP addresses, handsets

and intelligently analyse it…….

Intelligent Fraud Scoring

- Current Status
- Previous History
- Multiple occurrences across different accounts
- Suspicious locations – ‘fraud ‘hotspots’
- Unusual activity patterns



Qivox

False Positive Reduction

- White list geographic ‘safe areas’
- White list – known ‘good’ call forward numbers
- Watch list – ‘bad numbers, SIMs, locations
- Frequency of changes
- Network data – ported or upgrade?
- Temporal ‘disallowed’ periods

Results

- Reduce SIM SWAP and redirect fraud to ‘almost nothing’
- >96% success in obtaining network data
- Improves over time ‘learning product’

Active Checks

- One Time PIN
- Voice Biometrics

    Layered passive capability

        Gender
        Age
        Watch List
        White List

- Knowledge Based Questions
- Secret Questions

Volume

In UK today:-

Estimate 400,000 ‘risky’ bank transactions per day

15% might require VB back up

60K per day –

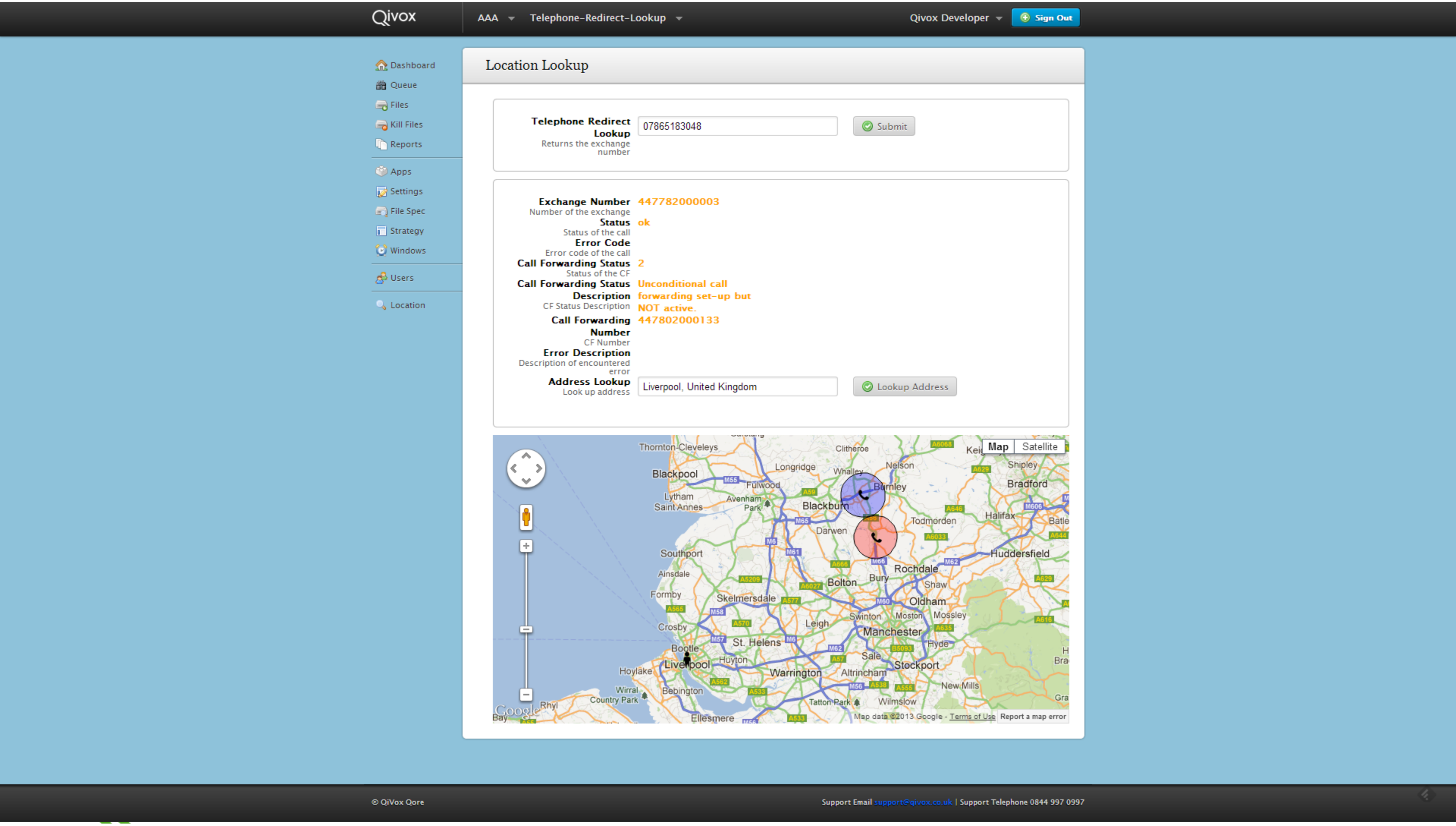
Demand 22m VB checks

Cf Telephone banking c.10m

Proximity Detection:- 4bn card transactions p.a.

Qivox

Proximity Correlation



Location Lookup

Telephone Redirect Lookup 07865183048 Submit
Returns the exchange number

Exchange Number 447782000003
Number of the exchange

Status ok
Status of the call

Error Code
Error code of the call

Call Forwarding Status 2
Status of the CF

Call Forwarding Status Description Unconditional call forwarding set-up but NOT active.
CF Status Description

Call Forwarding Number 447802000133
CF Number

Error Description
Description of encountered error

Address Lookup Liverpool, United Kingdom Lookup Address
Look up address

© QiVox Qore

Support Email support@qivox.co.uk | Support Telephone 0844 997 0997

Non-Banking

- Risky =

  Password reset
  Initial activation
  Change of details
  Allow third party access

  Volume per day – Google 10m/day
  Online marketplace – 1bn per day?

Qivox Fraud Services Includes……..

- Mobile and Landline Redirect
- SMS Forwarding
- SIM SWAP detection and analysis
- USSD
- CLI Spoofing
- Geographic Information
- Post transactional card fraud
- ATM and POS correlations
- And **Voice Biometrics**

THANKS

That’s all for today!

Qivox