

Human Behaviour and IT Security No Longer Need to Be In Conflict

Dave Vijzelman

Principal Solution Strategist Security



Innovation and Leadership

Cloud Authentication Leader

- 12 years experience
- Level 4 Saas
 - Multi-tenant, configurable
- Redundant data centers
 - PCI-DSS compliant
 - SAS 70 certified

Large User Base

- Over 150 million users
- 13,000 organisations
- Enterprises and consumer



Innovation and Technology

- Co-invented 3-D Secure
- Invented software strong authN
- Best-in-class risk management
- Tagless DeviceDNA
- Fraud Prevention Network
- Tokenisation – Format preserving encryption
- Over 35 patents

Partner Reach



Reselling
Arcot



IAM
Integrations



SaaS
Integrations



Arcot's Approach: 4 Observations



1. Threats are evolving

- Malware
 - Key Logger
 - Man in the Browser
 - Trojan
- Network infrastructure and social engineering
 - Man in the Middle
 - Phishing/Pharming
 - Challenge-Response interception / sniffing
 - Replay attacks
- Payment instrument attacks
 - Carding
 - Skimming/cloning
- Offline attacks
 - Physical device theft
 - Brute Force/Dictionary attacks



2. You cannot change human behaviour

“Over 50% users use the same user ID and password.”



“73 percent of Internet bank clients share online banking password with non-financial sites”.



“One out of five Web users still decides to leave the digital equivalent of a key under the doormat: they choose a simple, easily guessed password like “abc123,” “iloveyou” or even “password” to protect their data.”

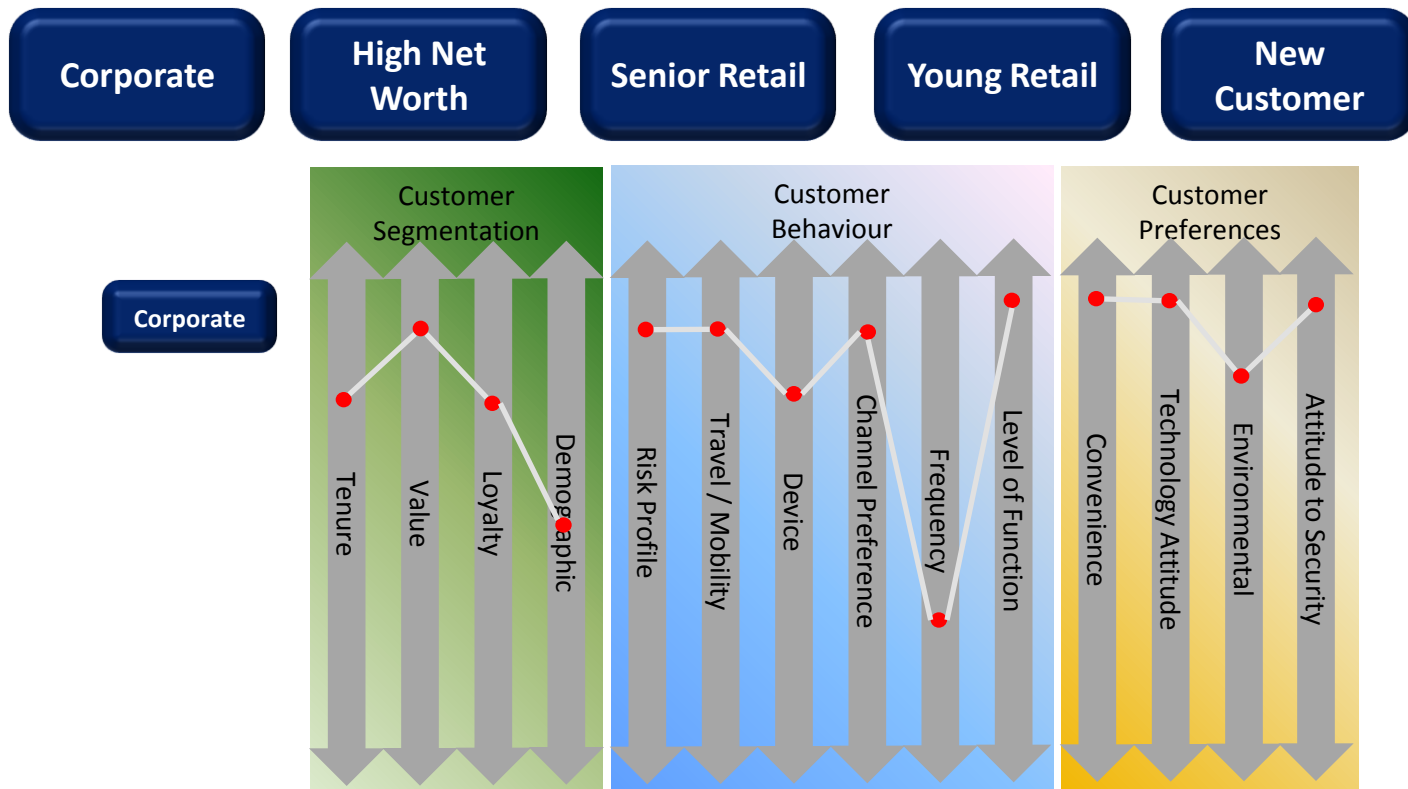
The New York Times

“Consumers Are Unwilling to Sacrifice Convenience for Security, Despite Widespread Online Fraud”



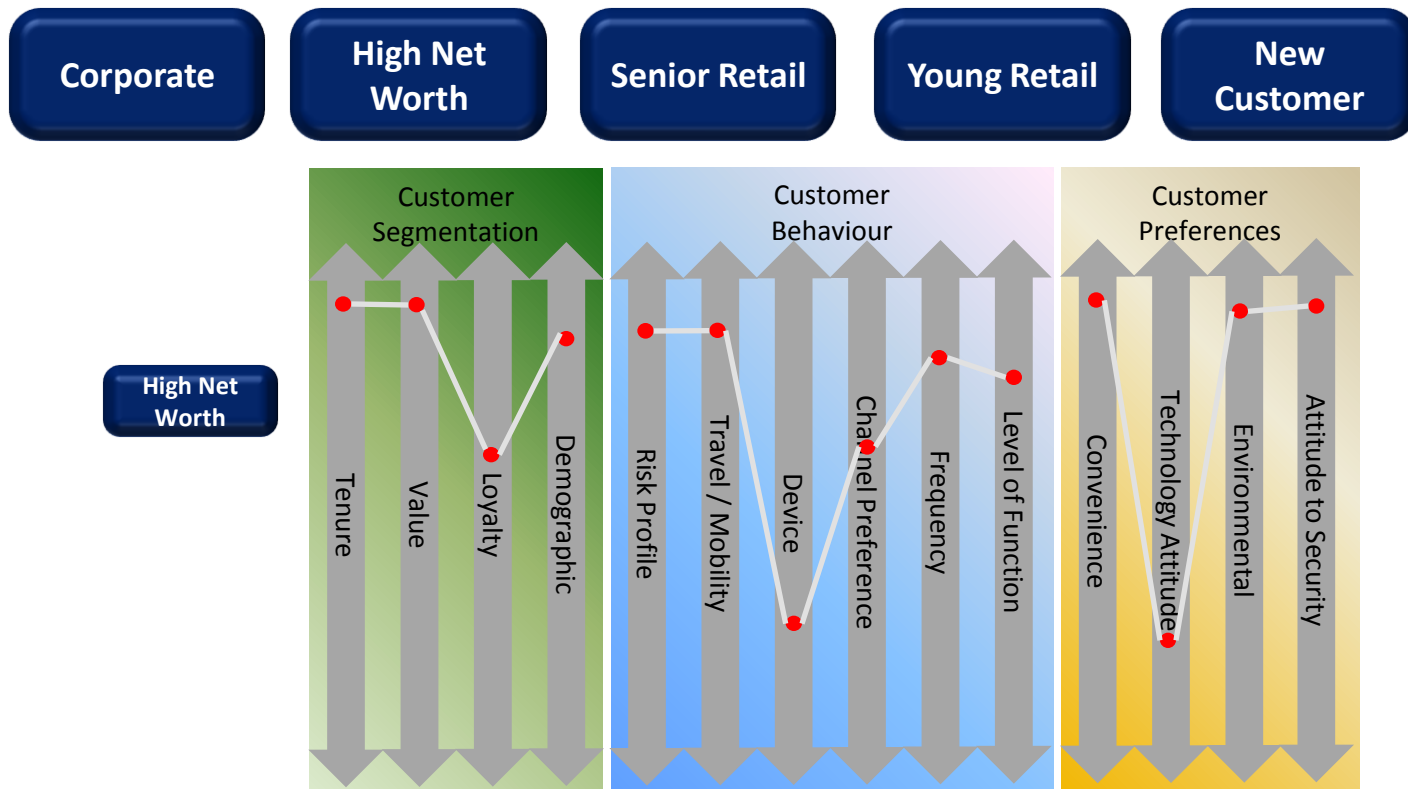
3. Users are not all the same: *'Living in our customers' world, not living in our world'*

- Segmentation – Value, Loyalty, Tenure, Demographic
- Behaviour – Travel, Transaction Frequency, Channel Preference
- Preferences – Security, Convenience, Technology, Environmental



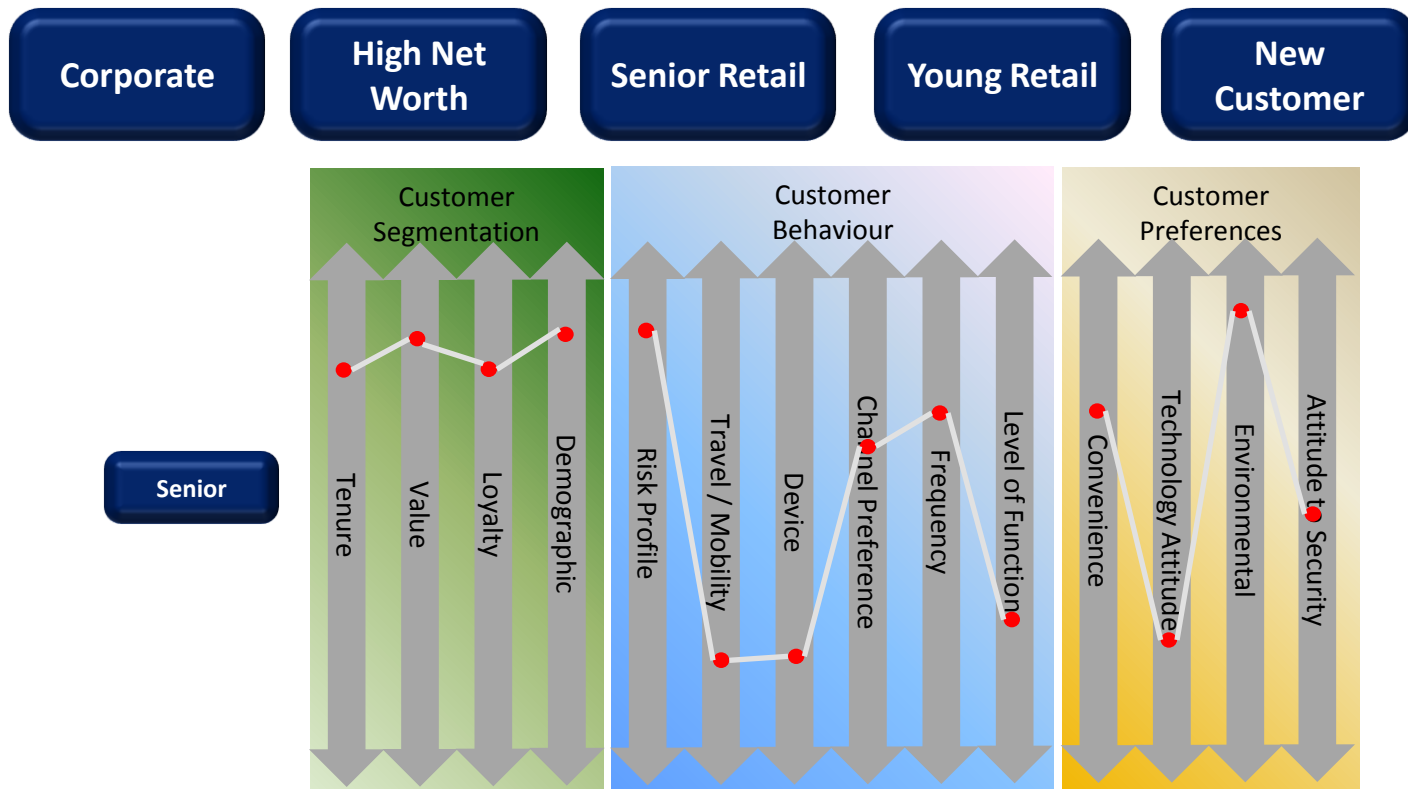
3. Users are not all the same: *'Living in our customers' world, not living in our world'*

- Segmentation – Value, Loyalty, Tenure, Demographic
- Behaviour – Travel, Transaction Frequency, Channel Preference
- Preferences – Security, Convenience, Technology, Environmental



3. Users are not all the same: *'Living in our customers' world, not living in our world'*

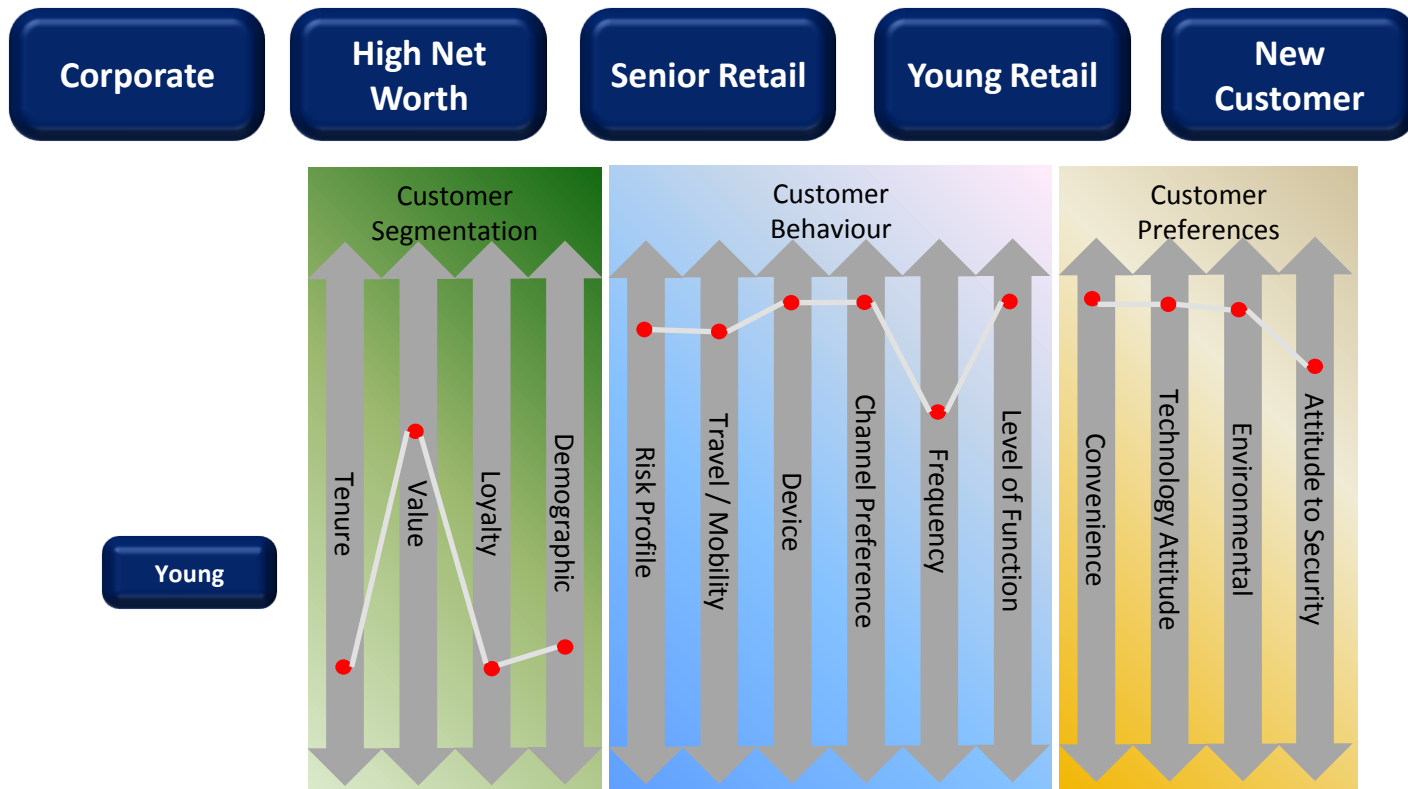
- Segmentation – Value, Loyalty, Tenure, Demographic
- Behaviour – Travel, Transaction Frequency, Channel Preference
- Preferences – Security, Convenience, Technology, Environmental



3. Users are not all the same:

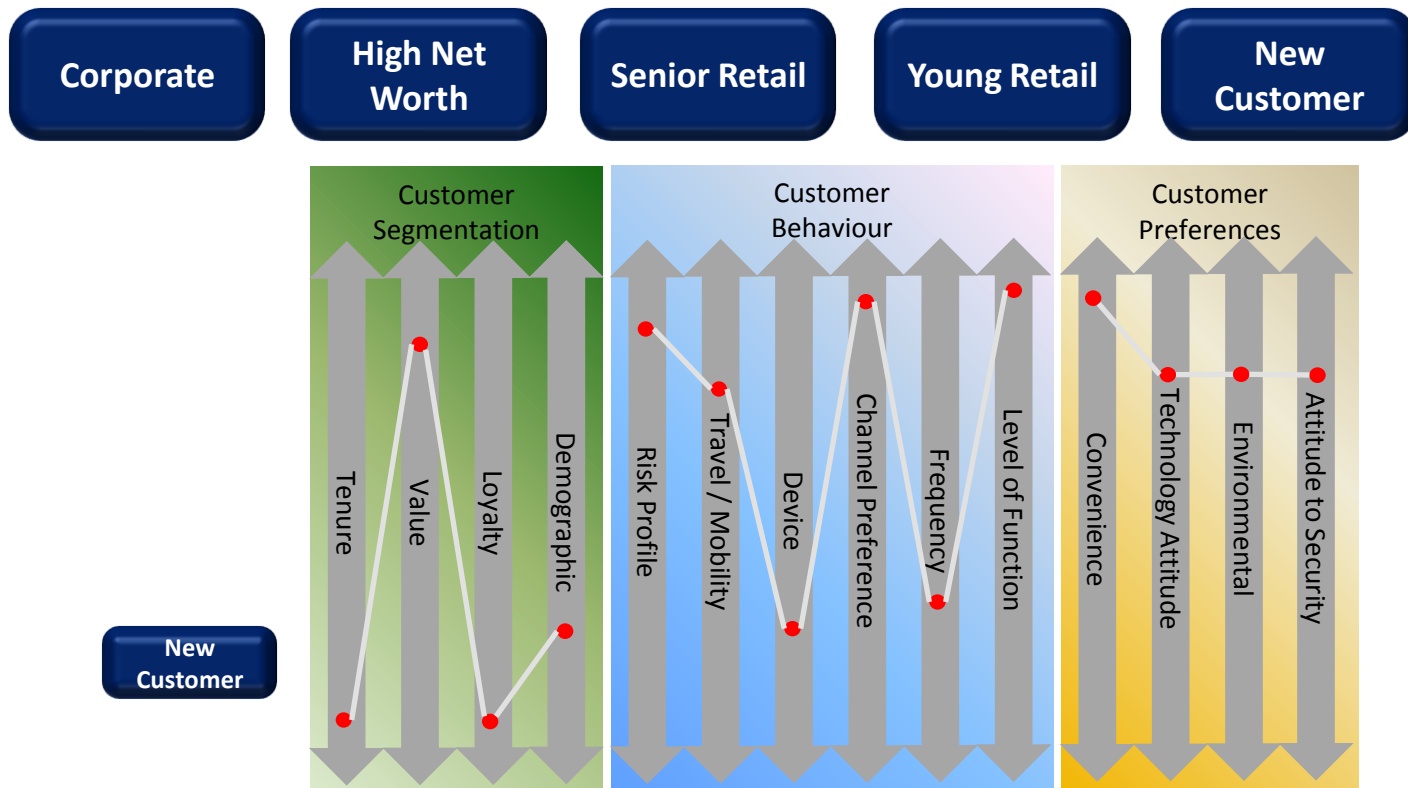
'Living in our customers' world, not living in our world'

- Segmentation – Value, Loyalty, Tenure, Demographic
- Behaviour – Travel, Transaction Frequency, Channel Preference
- Preferences – Security, Convenience, Technology, Environmental



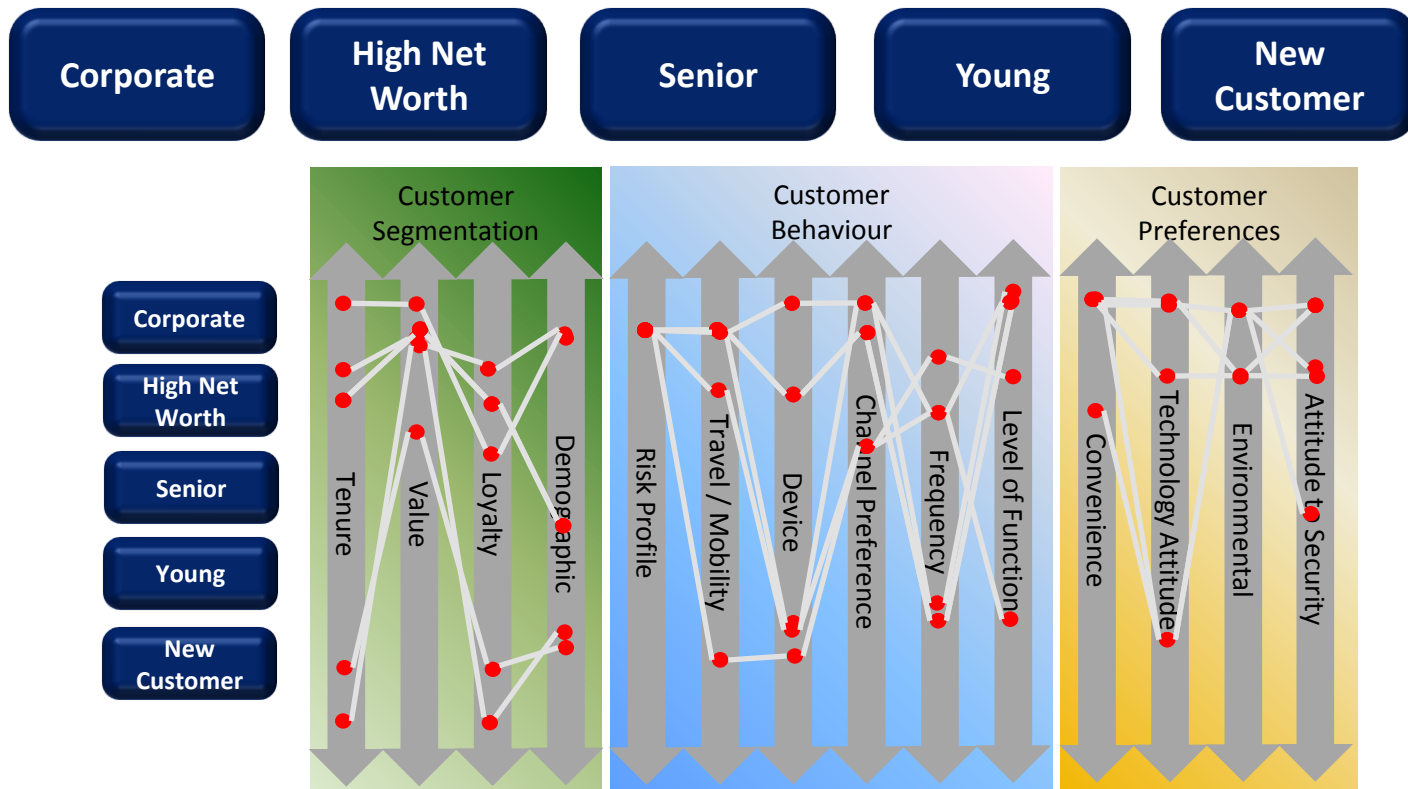
3. Users are not all the same: *'Living in our customers' world, not living in our world'*

- Segmentation – Value, Loyalty, Tenure, Demographic
- Behaviour – Travel, Transaction Frequency, Channel Preference
- Preferences – Security, Convenience, Technology, Environmental



3. Users are not all the same: *'Living in our customers' world, not living in our world'*

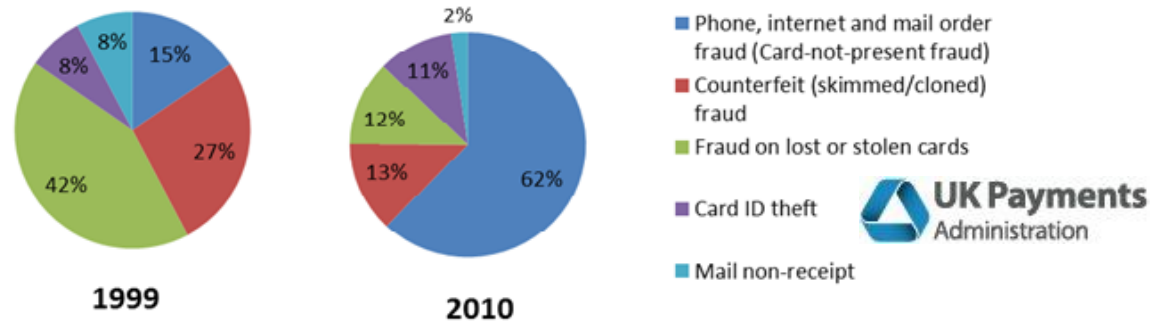
- Segmentation – Value, Loyalty, Tenure, Demographic
- Behaviour – Travel, Transaction Frequency, Channel Preference
- Preferences – Security, Convenience, Technology, Environmental



4. De-Perimeterisation & Consumerisation of IT

- Channels
 - Office/Branch
 - Internet
 - Telephone
 - Mobile
 - Employee
 - Written
 - Terminal/ATM
- Form Factor
 - Web-based
 - Apps
 - Social Media
 - Instant Messaging
- Delivery
 - Cloud
 - On Premise
 - Outsourced

Card Fraud Losses Split by Type (As percentage of total loss)



Arcot's Approach to Authentication

Increasingly Sophisticated Attacks and increasing rate of change



*Design layered solutions with **flexibility and nimbleness** in mind. There is no silver bullet.*

Customers are unwilling to compromise convenience for security



*Design **attractive and transparent** solutions that don't try to change user behavior*

Customers have different needs



Ensure that Authentication is appropriate for the user and context

Security, customer experience and opportunities are increased by 'protecting' all channels



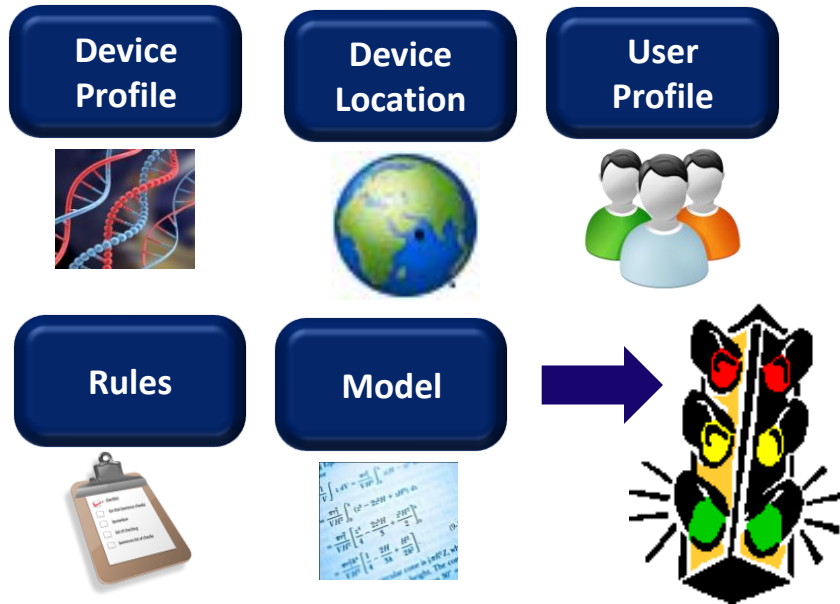
*Multi-channel **cost effective** solutions that are **easy to deploy & manage**. Authentication becomes a **business enabler***

Layered Approach: Secure Any Device from Any Location for Any User



Layer 1: Invisible Authentication

'More Secure and More Convenient Than A Password'



Invisible Risk-Based Authentication



Office / Branch

Internet

Telephone

Mobile

Employee

Written

Terminal / ATM

Example 1:

Organisation:

Bank

User Profile:

Retail & Corporate Consumers.

Activity: eCommerce

Business Requirement:

Maximise transaction success, minimise inconvenience, minimise fraud. Support any device.

Outcome:

95% transactions require zero authentication

1-2% transactions declined

3-4% transactions Step-Up authentication

Layer 2: Strong Authentication

'Greater Security With Zero Change To The User Behaviour'

Patented Authentication



One time password solution supported on all major device types

2FA delivered with a user name and password experience



Widest Support for Authentication

- Password/Partial/KBA
- OTP (multi-channel)
- CodeSure Cards
- CAP Readers
- OATH Tokens
- Open Standards



Strong / Appropriate Authentication



Invisible Strength



Industry Approved



Office / Branch

Internet

Telephone

Mobile

Employee

Written

Terminal / ATM

Example 2:

Organisation:
Telco

User Profile:
Global Employees

Activity:
All Online business activity

Business Requirement:
Travelling and local users on all devices

Outcome:
Secure and convenient access for all users from all devices

Layer 2: Strong Authentication

'Greater Security With Zero Change To The User Behaviour'

Patented Authentication



One time password solution supported on all major device types

2FA delivered with a user name and password experience



Widest Support for Authentication

- Password/Partial/KBA
- OTP (multi-channel)
- CodeSure Cards
- CAP Readers
- OATH Tokens
- Open Standards



Strong / Appropriate Authentication



Invisible Strength



Industry Approved



Office / Branch

Internet

Telephone

Mobile

Employee

Written

Terminal / ATM

Example 3:

Organisation:
Bank

User Profile:
Retail & Corporate Consumers

Activity:
Internet Banking

Business Requirement:
Customer mix includes mass retail, ultra-high net-worth consumer, high value corporate. Support any device. Need to open up online access and give convenient access whilst protecting significant assets

Outcome: Achieved customer satisfaction and fraud protection

Layer 3: Transaction Authentication

'Allowing Secure Transactions With an Insecure Device'

Transaction Authentication



Transaction Signing

Virtual Private Session

EndPoint Security

Out of Band



Office / Branch

Internet

Telephone

Mobile

Employee

Written

Terminal / ATM

Example 4:

Organisation:
Bank

User Profile:
Retail Consumers

Activity: Funds Transfers

Business Requirement:
Assume the user device is hostile, i.e. contains virus/malware but need to support high value funds transfers

Outcome: Achieved customer satisfaction and fraud protection



→ Account Management

Change Profile
Change pin
Preferences

→ Transactions

Transfers
Withdrawals
Pay Bills
Stop Payment

→ Other Services

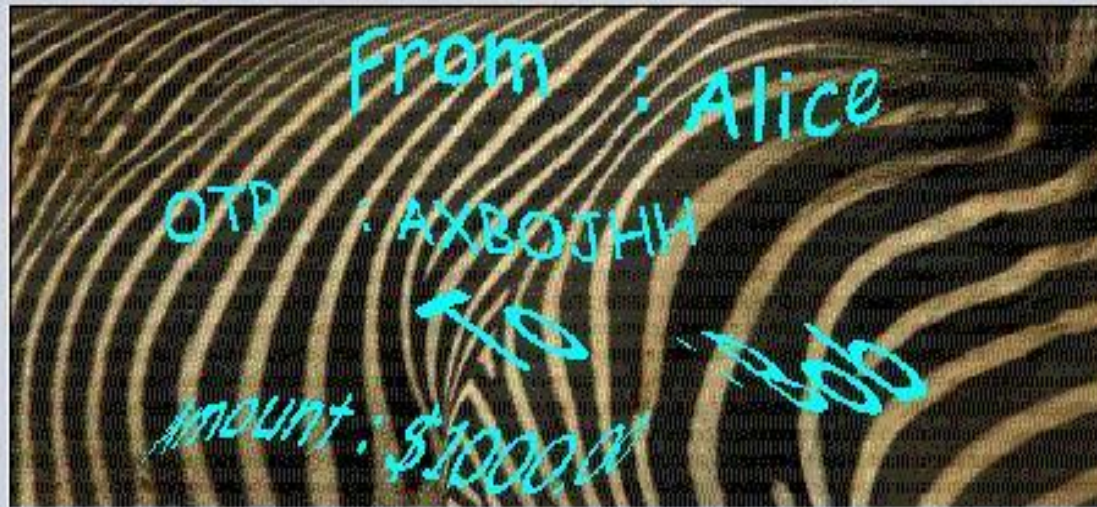
Investment Center
Loan Center
Retirement Center

→ Contact Us

Online Help
Contact Information

Funds Transfer Confirmation

Check your transaction details and then enter the one time password in the text box below.



Enter OTP from image:

Cancel

Continue

Layer 4: Beyond Authentication 'Turning Security Into a Business Enabler'

Document Authentication

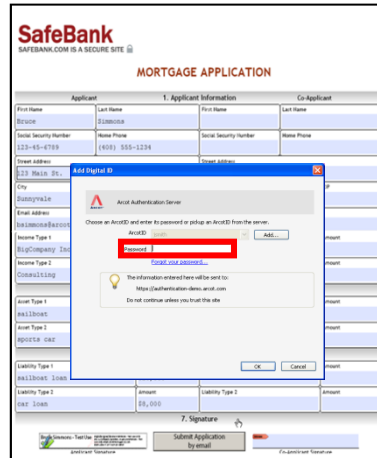


D

Outbound

D

Inbound



Office / Branch

Internet

Telephone

Mobile

Employee

Written

Terminal / ATM

Example 5:

Organisation:
Bank

User Profile:
Retail Consumers

Activity: Electronic documents bank-to-consumer and consumer-to-bank

Business Requirement:
Replace paper from bank to customer (statements, terms and conditions changes,) and from customer to bank (application forms, change of circumstances) to support any device

Outcome: Huge operational savings, improved customer convenience, environmental benefits

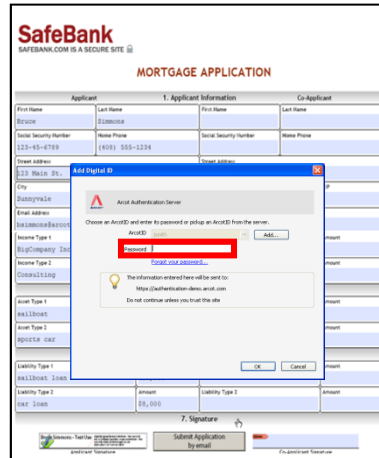
Layer 4: Beyond Authentication 'Turning Security Into a Business Enabler'

Document Authentication



D Outbound

D Inbound



- Templates
- Converters
- Filters
- Policies
- Encryption
- User Preferences
- Scheduler
- Logging
- Reporting
- Metering/Billing



Office / Branch

Internet

Telephone

Mobile

Employee

Written

Terminal / ATM

Statements/Notices
Bills
Alerts
Marketing Message
Photos
Audio/Video

Email
Browser
Mobile Apps
Facebook
SMS
Print



Layered Strategy for Preventing e-Fraud

Document Authentication



Transaction Authentication



Strong / Appropriate Authentication



Invisible Risk-Based Authentication



Office / Branch

Internet

Telephone

Mobile

Employee

Written

Terminal / ATM

- Full control over Rules & Policies
- Highly Granular – to user level
- Multi-Institution
- Common Reporting & Case Management
- Integration with other Systems
- Hosted or In-house (or combination)

Summary

- Fraud is becoming increasingly sophisticated, organised and complex
 - Fraud protection strategies should be risk-based
 - Authentication should be appropriate
 - Build in the ability to respond to threats and opportunities
 - There is no silver bullet – layers work best
- Customer Convenience
 - We don't try to change human behaviour
 - Flexibility to accommodate all user types and devices
 - Provide invisible security where possible
 - Make security attractive to the user
 - Use the additional security to provide additional value to the user
- Holistic Approach
 - Understand customer behaviour across all channels
 - Use the greater understanding of behaviour to better serve the user and this increase revenues, satisfaction and loyalty

You can provide different solutions for different users/scenarios/devices and add/change over time in response to opportunities and threats without needing to 'rip and replace'

Fraud protection with excellent customer experience is absolutely achievable in a few straight forward steps

CA Technologies

Enterprise Security Management technologies



Business Need

Manage and govern identities and what they can access based on their role

Control access to systems & applications across physical, virtual & cloud environments

Find, classify and control how information is used based on content and identity

Capabilities

- Identity Management and Governance
- Role Management
- Provisioning
- User Activity & Compliance Reporting

- Privileged User Management
- Virtualization Security
- Web Access Management
- Web Service Management
- Federation

- Information Discovery
- Classification
- Data Policy Management

Content Aware Identity and Access Management

Thank you

For more information contact:

Dave Vijzelman

email: dave.vijzelman@ca.com

Tel: +32 476878584

