

# Identity Theft

*A Risk To Be Managed*

**Richard Parry**  
**SVP, Fraud Risk Management Director, Consumer**



10 February 2005

## Discussion Topics

- **The symbiotic relationship between new products and product delivery methods**
- **Changes in consumer behavior and their impact**
- **The importance of authentication**
- **Traditional authentication approaches fail to support banking behavior today**
- **Managing fraud at the customer level**
- **Impact on tool design and functionality**
- **The consequences of reaction over remedy**
- **Recommendations for the future**

## **360<sup>0</sup> View on Fraud**

- |                       |  |
|-----------------------|--|
| <b>1977 - 87</b>      | <b>Royal Hong Kong Police Force</b><br><i>Chief Inspector, Commercial Crime Bureau</i> |
| <b>1987 - 95</b>      | <b>Visa International (Asia Pacific)</b><br><i>Senior Manager, Risk Services</i>       |
| <b>1995 - 01</b>      | <b>Citibank N.A.</b><br><i>Fraud Risk Management Director - Global Consumer</i>        |
| <b>2001 - 02</b>      | <b>Visa International (Asia Pacific)</b><br><i>General Manager, Risk Management</i>    |
| <b>2003 - Present</b> | <b>JPMorganChase</b><br><i>Fraud Risk Management Director - Consumer</i>               |

# Fraud and Identity Theft

- **Lack of a public agenda focusing on the true causes of identity theft**
- **Cause-and-effect generally misunderstood**
  - **Stoking indignation**
  - **Identity theft often confused with fraudulent-use-of-account**
  - **Ad campaigns and “authoritative reports” confusing identity theft with fraudulent use of account**
  - **Definitions matter!**

## Definitions Matter

- **What you call it determines how you fix it!**
- **Identity Theft is when a thief assumes someone's identity by using personal information, such as his/her name, social security number, and date of birth to borrow or buy in the genuine person's name, or even commit crime in their name**
  - ***Leaving the victim with the bills and a damaged credit history***
  - ***And perhaps an arrest warrant or criminal record***

# Account takeover

- **Account takeover of existing accounts**
  - **Through counterfeit ID and/or access to passwords and personal particulars**
  - **Assumes control over someone else's financial accounts**

## Identity Theft *is not*

- Using someone else's credit card number to buy
  - Goods and services
  - Over the internet
  - By phone or mail order
- This *is* fraudulent use of their *account*

# Identity Theft

## ■ Cause

- **Compromise or giving away of sensitive identity information enabling the thief to pose as the real person (victim)**

## ■ Remedy

- **Tighter control of personal information distribution (customer)**
- **Security of customer data (internal)**
- **Improved customer verification prior to new account opening**

# Fraudulent-use-of-accounts

## ■ Cause

- **Compromise of transaction data stored on merchant, retailer's and ISO's databases**

## ■ Remedy

- **Enforcement of payments industry data security standards at all card accepting retailers, end-points, switches and network connections**

# Customer Impact

## ■ Identity Theft

- Time and expense re-establishing credit worthiness and personal credibility
  - Financial Institutions absorb financial loss

## ■ Fraudulent Use of Account

- One or two phone calls in most cases
- No impact to credit history
- Card replaced within days
  - Financial Institutions absorb financial loss

## What the Consumer Says.....

- There are too many PINs and passwords in our lives
- Security is important to me!
- Identity Theft and fraudulent-use-of-account are the same thing
- The lender is responsible
- How could a bank let someone else open an account in my name?
- My social security number is my identity!
- State driving licenses are as good as an identity card!
- We are treated like criminals when bankers try to distinguish the real victim from the identity thief
  - “Why couldn’t you do this (level of verification) before you let the crook open an account in my name?” (Actual quote from a victim)

# Customers and Security

- Customers want their security to be:

- Fast
- Cheap
- Simple
- Unintrusive

} Nothing wrong with that!

- And very secure!

- But will customers pay for the level of security they demand?

- User-select PINs and Passwords ensure that the shared secret will always be a flawed authentication feature

- Who *really* uses different PINS and Passwords for each ATM, phone and Internet channel to each financial service provider they have a relationship with?

# Customer Behavior

- Consumers are *conditioned* to reveal information about themselves
  - When signing up for all manner of services, surveys, discounts, cash backs, “freebies” and offers
    - Including the warranty form for that new shredder!
  - Without regard for where the information goes, where it is stored, by whom, for how long, or who has access to it!
  - Banks and financial service providers are deemed *accountable*
  - Even though their authentication strategies are made vulnerable from this trusting attitude about personal information

## Where Liabilities Lie

- **Customers are not liable for fraud resulting from fraudulent-use-of-account**
  - **Consumers have no stake in putting legislative pressure on retailers, vendors and non-bank custodians of data to adequately secure personal information that creates vulnerability to both identity theft *and* fraudulent use of accounts**
- **But financial institutions bear the brunt of reactive legislation and regulation and consumer indignation**
  - **Financial institutions must protect themselves from their customer's behavior**

## **Some Self Correction is Happening**

- **Awareness is changing the landscape**
- **The credit bureaus and most banks have introduced assistance strategies to help victims rehabilitate their credit report standing**
- **Financial service providers are rethinking and improving verification strategies**
- **Many consumers are becoming cautious about revealing personal data**
- **Solution vendors are bringing innovative products to market to help improve authentication**

## Still a Long Way to Go

- **The time it takes for victims to rehabilitate their credit standing is getting shorter**
  - **For *most* victims – not *all*!**
  - **Still an emotionally draining experience**
- **Account Takeover remains especially vexing**
  - **Requires robust, cost effective customer authentication to remedy**
  - **Remains vulnerable to consumers' failure to keep shared secrets and use different secrets for different activities**

# Customer Authentication

- **Most practices fall into one of two types**
  - **Two pieces of information**
    - **Unique identifying particular or combination of particulars, such as name, User ID or Account Number**
    - **A shared secret - PIN or Password**
  - **Out of Wallet Questions**
- **Both dependent upon information remaining private**

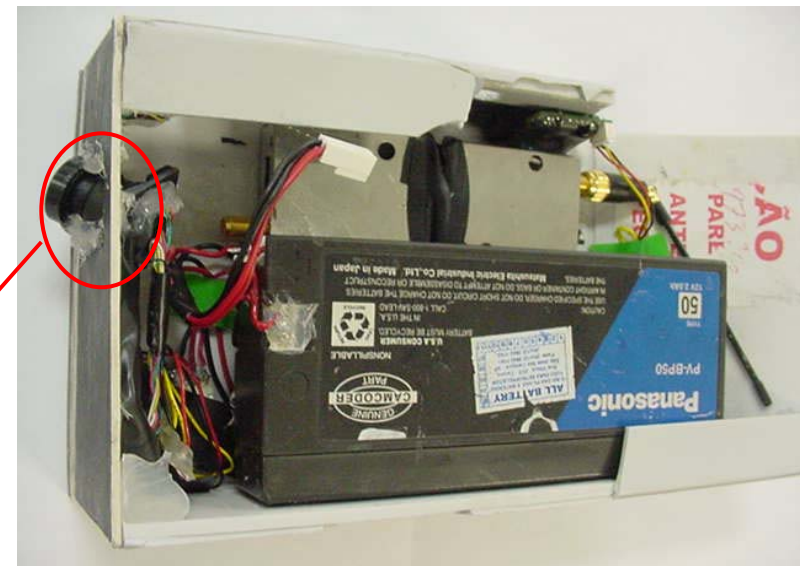
## **PINS Serve Us Well! – Don't They?**

- **PINS have been an effective authentication method for much of the past 35 years**
  - **PINS were first used at an ATM embedded in the wall of a bank - when cards were difficult to copy**
- **Then came user-select PINS**
  - **Customers could use the *same* PIN for every card in their wallet**
- **PIN went to the point of sale in PIN based debit networks and many use them as online passwords**

# ATM Environment



- False fronts on ATM terminals with built in magnetic stripe readers.
- Hidden camera captures PIN and transmits the information to a nearby crook
- Increasingly common



## ATM – Environment – Cont'd




- **Sniffing** devices installed in ATMs are another example of how a fraudster can compromise the ATM or Debit card PIN. In this example, the PIN and magnetic stripe information are captured before encryption.
- Recent cases have Bluetooth transmission to remote receiver.

## And An Old Favorite – “The Skimmer”


- This device can capture over 2500 credit card account numbers, expiration dates and CVV codes in the palm of your hand.
- The unit can operate continuously for 40 hours on a single 3V battery (6000 swipes).
- Skimmed data can be downloaded to any PC with software provided.
- At a moment’s notice, or the moment of arrest, the contents can be deleted with the press of a button to avoid prosecution.
- Cost = \$500



# Where Can I Get One? Where Else!



[home](#) | [pay](#) | [register](#) | [sign in](#) | [services](#) | [site map](#) | [help](#) <sup>?</sup>

[Browse](#) | [Search](#) | [Sell](#) | [My eBay](#) | [Community](#) Powered By 

[Back to home page](#)    Listed in category: [Computers & Electronics](#) > [Gadgets & Other Electronics](#) > [Other Gadgets](#)

---


## SMALLEST PORTABLE MAGNETIC STRIPE CARD READER

Item number: 3063217792

**You are signed in** [Watch this item](#) (track it in My eBay)

This is a private auction. Your identity will not be disclosed to anyone except the seller. If you are already bidding on this item, [view your bidder status](#). [Learn more](#) about private listings.

---



[Go to larger picture](#)

Starting bid: **US \$499.00**

[Place Bid >](#)

Time left: **1 days 15 hours**  
10-day listing  
Ends Dec-13-03 05:02:22 PST  
[Add to Calendar](#)

History: [0 bids](#)

High bidder: User ID kept private

---

**Buy It Now** Price: **US \$499.00**

[Buy It Now >](#)

---

Location: **Miami, FL**  
United States

### Seller information


[tssdenterprises](#) (80 ★)

Feedback rating: 80  
**Positive feedback: 100%**  
Registered Aug-15-02 in United States

[Read feedback reviews](#)

[Ask seller a question](#)

[View seller's other items](#)

 **Buyer Protection Offered**  
[See coverage and eligibility](#)

## And Biometrics?

- **Business still deems advanced methods of authentication complex, immature and/or expensive for widespread deployment**
  - **Biometrics (iris scan, retina scan, fingerprint, voiceprint)**
  - **Integrated chip with offline PIN verification**
  - **Other emerging technologies**
- **Many consumers are uncomfortable with biometrics**
  - **Too invasive**
  - **“Government gets too much control in our lives”**
- **Most biometric solutions do not solve the issues associated with remote-channel access**
- **Who pays and how to optimize infrastructure?**

## Latest “Risk du Jour”

### ■ Phishing

- E-mails purporting to be from well known goods and service providers, requesting personal information to “ensure” renewal/continuation of service

### ■ Spoofing

- Setting up bogus web sites that look like familiar legitimate sites
- Spurious solicitations for goods and services trick consumers into giving up data

### ■ Combinations of the two

## Why “Risk du Jour”?

- **Phishing and Spoofing is just traditional social engineering using new delivery channels**
  - **Great product development by thieves**
    - **Can be accomplished off-shore**
    - **Low risk**
    - **Low cost**
- **A compelling reason to rethink how we view the behaviors we’ve created around account access, authentication and fraud detection**
- **The present wave of indignation won’t address the causes**


**But the attempts do look pretty good.....**



December 18, 2003

**Online Demo**  
To learn more about our services, try our Demo.

**Important**  
Please login to check if your account is active. All BankOne accounts were disabled recently due to system update. [More Information](#)



Home equity lines of credit...Apply now and enjoy no annual fee. [Learn More.](#)

**Login**

Login [? What's New](#) [? System Availability](#) [? Help With This Page](#)

**Login:**

<b>User ID</b>	<input type="text"/>	<input type="checkbox"/> Save User ID on this computer
<b>Password</b>	<input type="password"/>	
	<input type="button" value="Log In"/>	

**Note**

**Due to system update please login to check if your account is still active. In case of inactive account please contact Bank One customer support center or enroll again.**

- User IDs and Passwords are case-sensitive.
- Do not use your browser's "Back" button to navigate once you have logged in. Doing so may cause your transactions to be submitted incorrectly.
- Forgotten your User ID or Password? [Restore your access.](#)

**Enroll**

To enable online access for your accounts, click the "Enroll Now" button.

To learn more about free services available from Bank One Online®, try our [Demo](#).

```
<INPUT TYPE="BUTTON" CLASS="bolAField1"
onClick="Javascript:location.href='Javascript:bolFormActionUrl
(document.bolForm,'\https://www.bankone.com/bank/BolEnrollGetStart.aspx?
bolType=E\');document.bolForm.submit();' "
```

**“Spoofed” website:**  
Sent as the body of an e-mail to trick people out of their user ID and passwords

## But What were They *Really* After?

- The few respondents to the previous example had their User ID and Passwords changed promptly to lock out the thieves
  - There have been logins but *few* attempts to move funds - Why?
  - Assess the average balances, regular deposits, date and number of the most recent checks cleared
  - Find out enough to issue counterfeit checks drawn on the account while the Bank looks for the obvious

## **Phishing: The Authentication Wake-up Call**

- **“Phishing” and “Spoofing” changed how we rely on the Internet for sales, marketing and customer utility**
  - **Can we send e-mails to customers alerting them to fraudulent emails?**
    - **“Don’t trust suspicious e-mails, but trust this one!”**
  - **Can we send e-mail solicitations to existing customers inviting them to enroll for products and services via a hyperlink to our website requiring login and personal information updates?**
    - **Bill-pay enrollment!**

## What Does All This Tell Us?

- Phishing demonstrates that *whatever* the shared authentication secret is, consumers can be “duped” out of it
- Cross-selling, linked accounts, equity lines of credit, have sweetened the honey-pot for thieves
  - Account takeover increasingly means gaining access to the customer’s complete finances and lines of credit
  - Remote channel access provides the “keys to the kingdom” if compromised
    - Not just access to an individual deposit or credit card account.

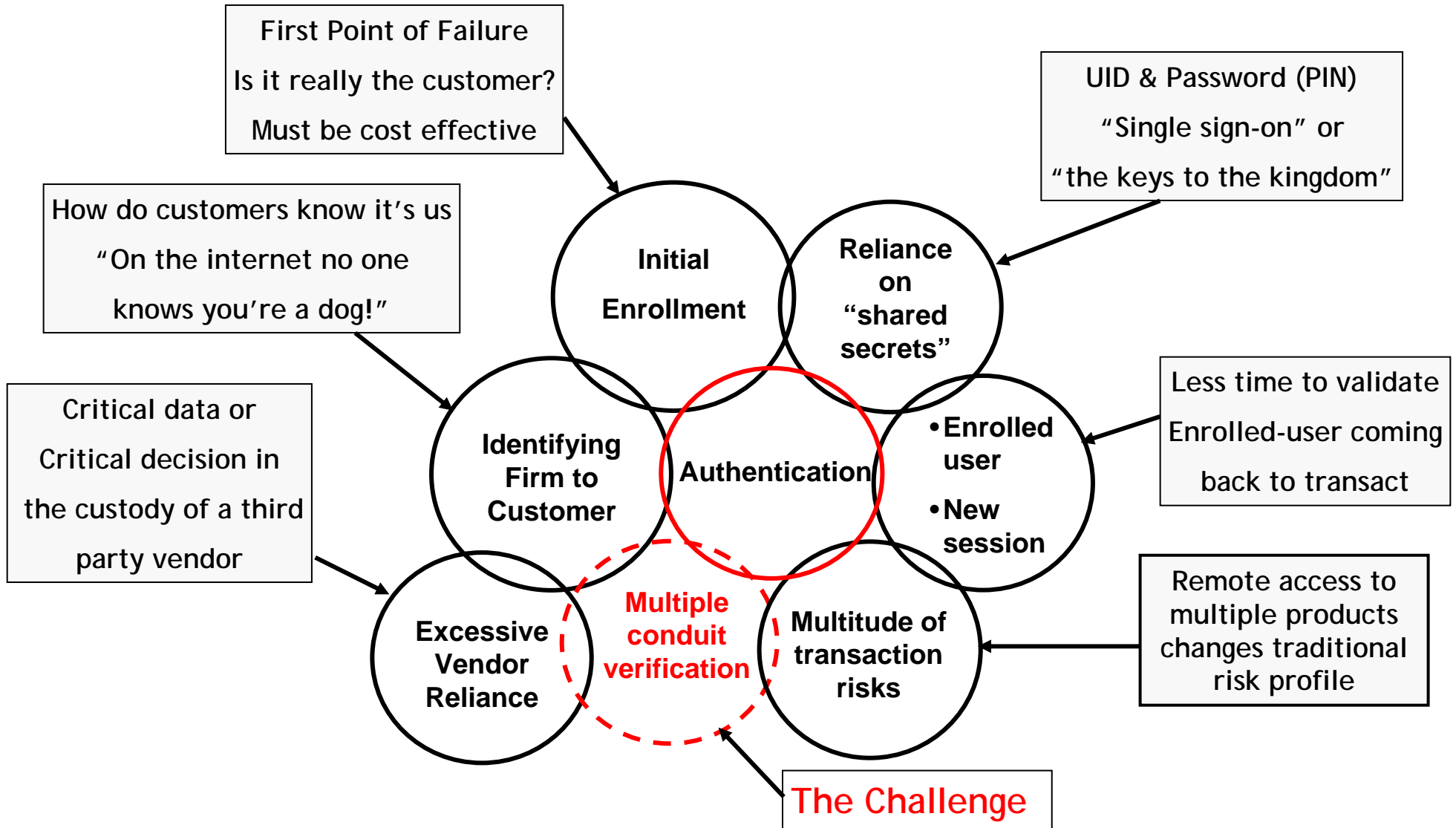
# The Changing Landscape

- **The way we do business has changed**
  - **So has the way our customers interact with us**
- **We have organizations that have served us well**
  - **Traditional control structures against familiar risks**
- **As circumstances change we tend to back new processes into traditional organizations**
- **A review of the changed landscape suggests a different approach**
  - **Organization should follow function**
  - **Changing functions will create unsettling but necessary new management structures**

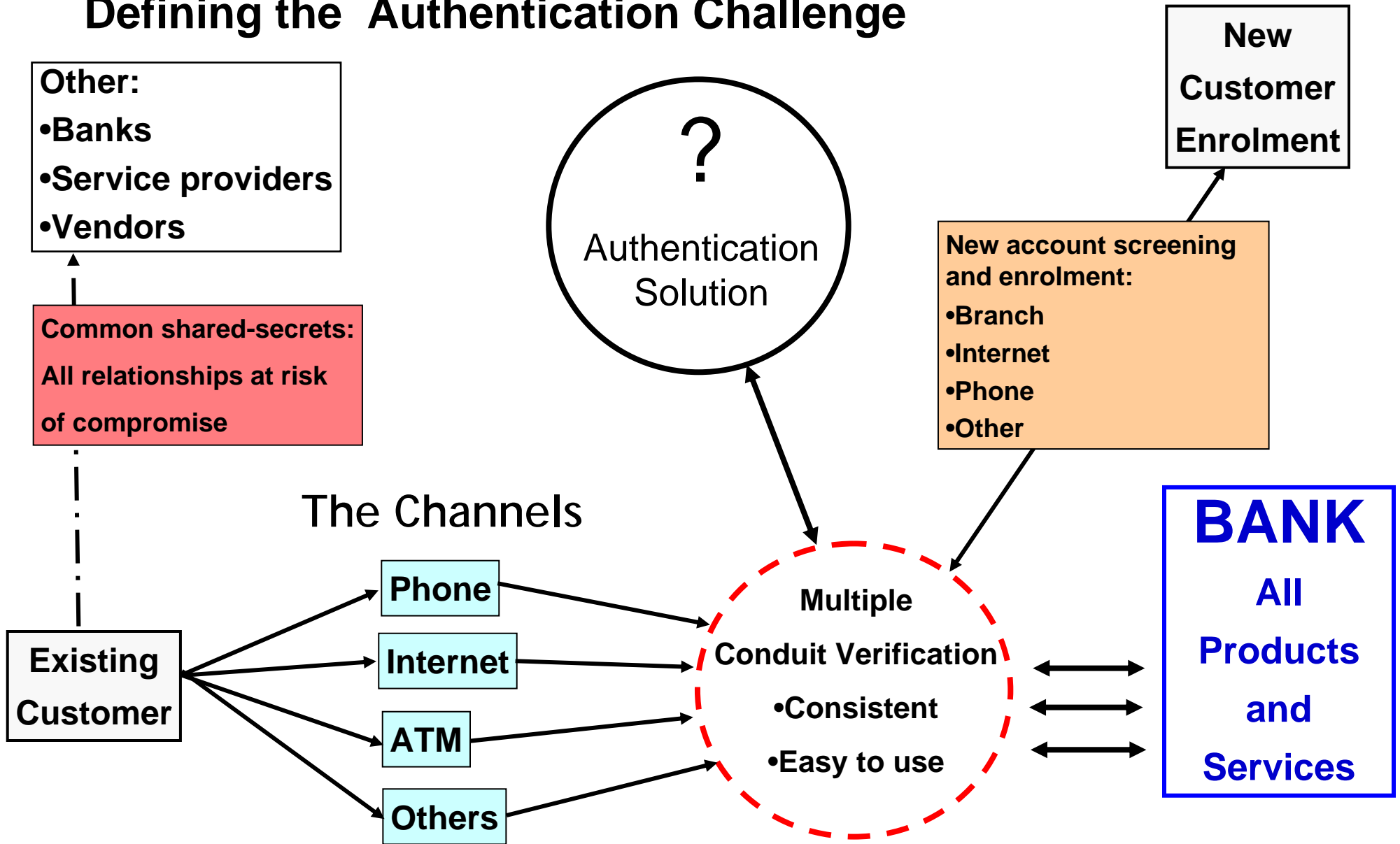
**So what does the new  
landscape look like?**

# Balancing Security and Convenience

## - Many Interdependencies



# Defining the Authentication Challenge



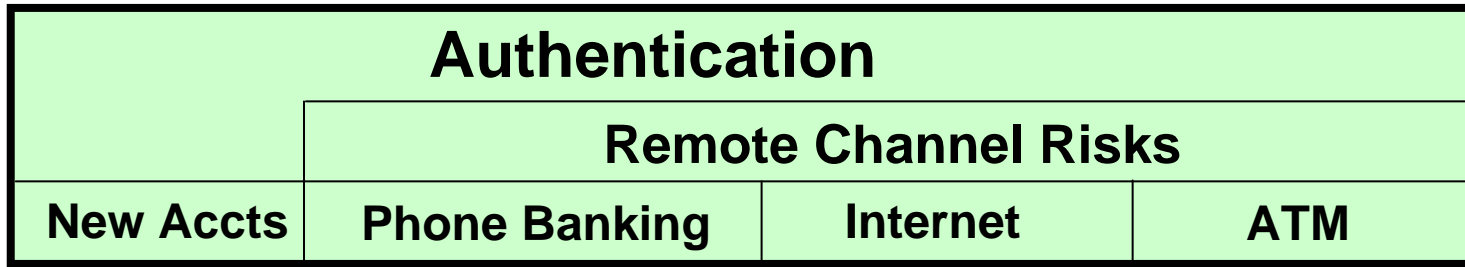
## A Complex Challenge

- Vendors must respond with innovative solutions
- Will consumers accept more robust authentication?
  - Attitudes may be changing
- Regulators and legislators can help with dialogue around solutions
  - Should a customer who does not avail himself of the authentication remedies of tomorrow be given total protection from responsibility from *consequential* fraud?
- Can we afford not to try?

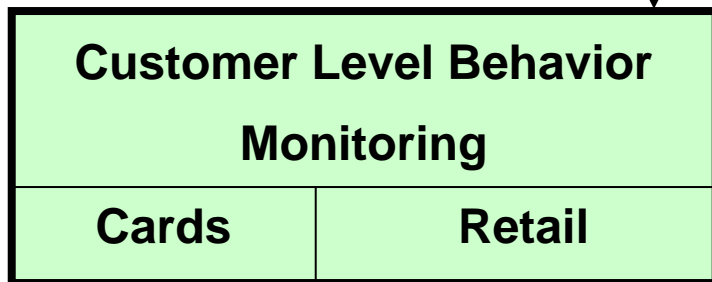
**And are banks ready to  
organize around the  
customer?**

# An Environment for Consumer Fraud Risk Management

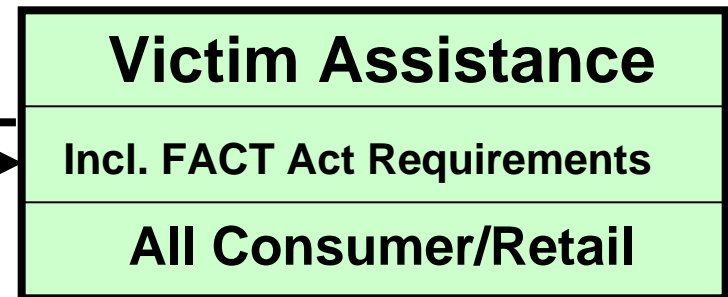
## Prevention



## Detection



## Cure



Info Exchange

Strategy: Risk Management  
Execution: Risk Operations



- Investigate employee malfeasances
- Pursue legal recovery
- Process defect analysis

# Where to Now?

- Engage consumers in a new dialogue about their role in authentication and security
  - Pay for the security demanded or go down the street for the cheaper/easier - less secure - option?
  - Who's responsible for making that choice?
  - Expect less (security)? Or, tolerate more invasive authentication practices
- Our industry must reconsider the implications of authentication on fraud prevention
  - Quality authentication cannot be allowed to be an area of competitive advantage
  - Nor can it strangle the business

# Thank you

## Discussion/Questions

**Richard A Parry**  
**Fraud Risk Management Director - Consumer**  
**Consumer Risk Management**  
**JPMorganChase**

**Tel: +1-312-732 4887**  
**E-mail: [richard\\_a\\_parry@bankone.com](mailto:richard_a_parry@bankone.com)**