University Bank

Email based identity theft, phishing and spam. What is the banking industry doing?

Stephen Lange Ranzini
President & Chairman, University Bank &
Michigan Business Development Company
U.S. Delegate to UN CEFACT TBG5 (Finance)
U.S. Observer to ISO TC68 (Financial Services)
Member, X9 (USA ISO ASC) Board of Directors
Chair, Marketing Committee of NACHA's EBIDS Project
Member, FSTC Security Committee &
FSTC Counter-Phishing Project Steering Committee
☎(734) 741-5858 xt 226
✉ ranzini@university-bank.com

With assistance from Michael M. Talley

Dec 2004 ISPAB

University Bank

What's Wrong With This Picture?

"On the Internet, nobody knows you're a dog."

University Bank

ID Theft & Privacy Solution

- Strong two factor authentication is necessary to solve the ID Theft crisis as well as roll out next generation web services for:
  - Security
  - Payments
  - Compliance
  - Privacy enhanced & piracy protected information services
- ...but are the dogs willing to eat the dog food?
- We can entice customers with a revenue mix offering free federated identity management services for email spam blocking and charging for other federated identity management services & web services
  - Up-sell users fee services from free services
  - Free services are a hook to increase market adoption of fee-based federated identity management services

Questions?

Michael M. Talley

Lead Independent Director & Audit Committee Chairman, University Bank

Chairman, FSTC's Council for Community Banks & Member, FSTC's Security & Business Continuity Committees

☎(212) 364-3454

✉ mtalley@ladenburg.com

Stephen Lange Ranzini

President & Chairman, University Bank

U.S. Delegate & Webmaster, UN CEFACT TBG5

U.S. Observer, ISO TC68

Board Member, ASC X9

Member, FSTC's Security & Counter-Phishing Steering Committees

☎(734) 741-5858 xt 226

✉ ranzini@university-bank.com

University Bank

Who *is* that guy?

- Graduate of Exeter & Yale
  - Scholarship student
- Convinced BankOne to lend me the money to buy a bank in a leveraged buyout
  - At age 23
- 16 years later still President & Chairman of University Bank
  - Founded seven financial services businesses from scratch
- President & Chairman of Michigan Business Development Company
  - Mentored dozens of entrepreneurs
  - Over $275 million invested into these businesses
- Deeply involved in banking standards and security activities
  - ISO, UN CEFACT (ebXML under United Nations), X9

Standards Activities at University Bank

- Member of Financial Services Technology Consortium (FSTC)
- American Bankers Association (ABA)
- Independent Community Bankers Association. (ICBA)
- National Association of Corporate Directors (NACD)
- National Coalition for Advanced Manufacturing (NCAM)
- National Center for Manufacturing Sciences (NCMS)
- Accredited Standards Committee (ASC) X9, the U.S. standards setting body for financial services under ISO
- Int'l Standards Organization (ISO) Technical Committee 68 (TC68), the global standards setting body for financial services
- U.S. National Coordinator for United Nations Centre for Facilitation of Trade and Electronic Business, International Trade & Business Processes Group, Working Group 5 Finance Domain (UN CEFACT TGB5), the global XML standards setting body for financial services under the UN

University Bank

OECD meeting findings (3)

- In first half of 2004 between 1 in 10 and 1 in 14 of all emails globally were viruses.
- More ominously, every virus launched this year has a zombie network back door, or "Remote Access Trojan" (RAT).
  - !!! The latest version of RATs also are enabled with software that allows the RATs to load additional software to compromised PCs, creating networks of zombie PCs called Zombie Bot Networks.
  - !!! The newer Next Generation RAT key loggers are down to just 2 kilobytes in size.
- 30% of all users are harboring RATs. This would mean that 200 million PCs globally (30% of the 665 million global email users) are controlled by RATs.
  - → Potentially up to 30% of all PC users who use Internet banking or Online Stock Brokerage services are also compromised.
- The successful denial of service attacks against Akamai and Google earlier this year were launched via Zombie Bot Networks.
  - → (source: MessageLabs)

University Bank

OECD meeting findings (2)

- In July 2004, fully 94.5% of all email globally was junk email.
- Global statistics indicate that junk email levels in Asia/Pacific are much lower but rising rapidly and they predict that they will catch up in six to nine months.
- This also means that U.S. levels of junk email are much higher than the global average.
  - (source: MessageLabs)

University Bank

OECD meeting findings (1)

- Year-to-date ending July 2004, there have been 3 trillion junk email messages versus 1.6 trillion for the entire year of 2003, at a global cost of $107 billion to $131 billion per year.
- At the current rate of increase, by December 2004, the annual global cost of junk email messages will rise to $200 billion.
  - (source: Sophos)

Banking Infrastructure Projects and Participations

- Member, FSTC Security Committee
- Member, FSTC Payments Committee
- Member, FSTC Counter-Phishing Project & Steering Committee
- Participant in FSTC Security Committee Liberty Alliance/SAML Report
- Member, FSTC/GSA Federated Identity Management Project
- Chair, FSTC's Council for Community Banks
- Liaison to: SIMC, (Security Industry Middleware Council)
- Liaison to: CSIS, (Center for Strategic & International Studies.
- Chair, Business Development Committee of the National Association of Automated Clearing Houses (NACHA)'s Electronic Billing Information Delivery Service (EBIDS) Project
- Member, Ford Foundation Innovations Center for Banking, Technical Advisory Board

University Bank

OECD Findings (7)

- RATs impede successful prosecution
  - Two spammers in England got off on junk email related legal charges through the defense that while their computers did it, a Remote Access Trojan was responsible.
  - Since guilt must be proven beyond a reasonable doubt this appears to be a bulletproof legal defense.

University Bank

OECD Findings (6)

- Anti-virus vendors require an average of eight hours to update their software following each attack
  - Therefore every PC is vulnerable for the first eight hours of each attack.
  - A new PC connected to a cable modem Internet service such as that provided by Comcast, will be on average attacked within 20 minutes after being connected to the cable modem network.
  - The amount of time required to download all software patches from Microsoft required to fully protect a legacy PC versus compromise exceeds 20 minutes.
  - Therefore, it is unsafe for consumers to connect to a broadband network of any type with a PC that hasn't already been configured with all required software patches, firewalls and security upgrades.

University Bank

Phishing: Scope and future direction

- Zombie bot networks are the first commercial implementation of grid
  - Networks have 25x the computing power of the largest super computers
- Mass personalization now possible
  - RATs for Google input capture for detailed profiles
  - Detailed profiles are much more valuable
- Weakest links are attacked
  - Check fraud x2
  - ACH Web/Tel fraud x2
  - Mortgage origination ID theft fraud x2
  - World Bank says that electronic crime doubling every year since 1998
  - Estimate from World Bank that global ID theft cost to financial institutions is $222 billion per year
- Landing on a website with a browser could compromise a PC
  - 4,000 exploits identified in Internet Explorer in 2003
  - 4,000 more identified through 8/31/2004

University Bank

Economics of Spam & Phishing (2)

- The value of a stolen credit card number averages $100 in the black market
  - Only 80 credit cards need to be stolen each day to generate a profit for the malicious spammer.
- Each identity theft can cause between $2,000 and $10,000 in losses to consumers and banks.
  - The theft of an entire online identity via RATs could be worth $500 to $1,000 on the black market. Therefore, a RAT based identity theft would only need just 8 to 16 per day to generate a profit for the malicious spammer.
- The economics for the Zombie Bot Networks created by the RATs are much better:
  - $100 per hour losing on average 500 machines per day from their network
  - If the typical network has 100,000 compromised PCs, then the average half life of each network is 100 days
  - If each network is utilized 50% of the time the revenue averages $240,000 per network or per virus released into the Internet with a RAT.
- Excellent funding vehicle, attack vector and communications channel for terrorists

University Bank

OECD meeting findings (4)

- A majority of all junk email is now generated through these Zombie Bot Networks or open relays.
- The value of a compromised zombie PC grows dramatically if it is connected to a high-speed Internet network such as a broadband network.
- Therefore, cheap broadband Internet access is driving the growth of junk email, theft and the utility of Zombie Bot Networks.
  - (source: Symantec)

University Bank

Economics of Spam & Phishing

- Typical spammer:
  - 200 million junk email messages per day
  - Break-even at 400 purchases at $20 each to generate the $8,000 in revenue required to run the spamming system.
- Fully 28% of email users respond to junk email solicitations.
- 8% of email users have purchased as a result of an offer received from junk email.
  (source: Symantec)
- What do people buy through spam?
  - Computer software: 27%
  - Clothes and jewelry: 24%
  - Leisure and travel: 21%
  - Education: 14%
  - Drugs: 13%
  - Finance: 12%
  - Investments: 11%
  - Adult entertainment (e.g. porn): 10%\

  (source: BBC News)

University Bank

OECD Findings (9)

- OECD: What can you do now?
  - Internal misuse of corporate networks by employees to generate junk email is also on the rise.
  - To determine if your own network is a source of junk email, register with America Online's free Complaint Feedback Loop tool at http://postmaster.aol.com.
  - Open port 25 can allow unlimited spam.
    - Close all Port 25
    - Use Sendmail v8.9 or later
  - My opinion: These findings are of limited use
    - Did you really expect international government agencies to fix your problem?!

University Bank

OECD Findings (8)

- Spam over Internet Telephony, or "SPIT":
  - SPIT combines Voice over Internet Telephony, which allows very low cost phone calls internationally with technologies to spoof standard telephone caller ID technology
  - SPIT can be used to perpetrate a new type of lucrative Internet based fraud using standard telephones.
  - Consumers can now get a phone call at home, see Citibank as the caller on their Caller ID Box and be requested to reveal security codes & credentials.
  - These attacks can be fully automated using voice recognition software or overseas call centers staffed with live operators.
- Spam over Instant Messaging ("SPIM")

University Bank

What Can Be Done?

- International Telecommunications Union announced that the ITU is creating a register of anti-spam legislation and responsible agencies for enforcement.
  - It is available at http://www.itu.int/osg/spu/spam/law.html
- OECD is launching a Best Practices Took-Kit
- U.S. FSTC Banks and IT Vendors (www.fstc.org) have launched the Counter-Phishing Project:
  - Taxonomy of Phishing
  - Cost analysis work sheet template
  - Life Cycle Definition of Phishing
  - Catalogue of Solutions
  - Rating Criteria to Evaluate Solutions
  - Phase 2 Projects to test promising Solutions

Domain Authentication Technology to the Rescue? (2)

- Will Domain Authentication technologies even work?
  - Already 2.5% of all email globally is authenticated using one of the new four standards.
  - However fully 3% of all junk email is already authenticated under one or more of the proposed standards.
    - (source: MessageLabs)

University Bank

Reputation services to the rescue?

- Emerging consensus that reputation services are "The New New Thing"
  - However, .mail TLD proposal shows the flaws
    - mass personalization
    - zombie bot networks
  - ...enable means to defeat reputation services

University Bank

Domain Authentication Technology to the Rescue?

- Internet Engineering Task Force (IEFT) is formally considering several proposals for domain level authentication:
  - Cisco's Identified Internet Mail
  - Sender ID
  - Domain Keys
  - Microsoft's SPF
    - However, to be fully effective, these technologies must be universally adopted globally
    - One Internet pioneer at the OECD meeting in Korea predicted that it would take 5-10 years for these technologies to gain universal adoption.
    - Already, two powerful Internet organizations have come out formally against the adoption of any of these technologies because of their inherent limitations.

University Bank

What Can Be Done (2)

- Switch your browser to Mozilla Firefox
  - Merely landing on certain compromised websites using IE™ is dangerous
    - Thousands of mainstream merchants compromised
    - Deutschland eBay compromised
  - Security through obscurity
  - Available free at www.mozilla.org
  - Coming soon: Earthlink toolbar version
- Install active spyware blocking software
  - e.g. Spybot from www.pctools.com
- Sign-up for active email scanning service
  - e.g. MessageLabs
- Sign-up for active kernel activity pattern recognition software
  - e.g. Whole Security, Corillian

More Secure Microsoft Windows and IExplorer to the Rescue?

- Information Assurance for Trusted Computing costs a lot of money
- ...and if you issue a patch, the Information Assurance work needs to start over from the very beginning!
- Therefore, the solution must be that if the credentials are stolen they have no value
  - Strong 2 Factor Authentication:
    - What you Know
    - What you Have
  - Plus Where you are and When you are

University Bank

Is Identity Management Alone the Killer Ap?

- Beyond domain authentication, we could know individual identity through strong authentication
- What about the Khazakstan spammer?
  - We know who he is
  - It is legal for him to send 200 million spam per day
  - It is lucrative enough for him to pay off his gov't to ensure it doesn't change its policies
  - e.g. Morpheus peer-to-peer file sharing system
    - Incorporated in Khazakstan
    - Hosted in Nauru
  - On the Internet, everyone is your next door neighbor
  - 190 countries and identity theft is more lucrative than the drug trade, and safer for the criminal enterprise

University Bank

What Can Be Done? (3)

- The future killer ap: Email postage with SAML 2.0 Federated Identity Management?
  - **GSA/FSTC/EAI eAuth Project**
- We propose to create a new protected zone of the internet for First Class Email™
  - **User strong identification/authentication**
    - In order to send or receive an email you must be strongly authenticated by the bank of your choice
  - **Shift costs to spammers from recipients**
    - Sender must attach a valid electronic check for at least a penny to each email
      - cashable at the *option* of the recipient

- Please note: we have three patents applied for covering this business model and the technical methods to carry it out

University Bank

What Business Problem are we addressing (2)

- We can get paid a lot of money to solve these problems
  - Existing bank systems & their complexity are part of the problem
  - Value created:
    - $940mm to $1.560bn for First Class Email system hub
    - $1.1 billion +-$200 million for 10 master global bank licensees, or $9 to 13 billion total
    - Assuming 10% market share of the 665mm email users globally at the end of three years

University Bank

What Business Problem are we addressing?

- Annual costs we can reduce & get paid to lower:
  - Cost of email Spam: $200 billion
    - OECD (Group of 30) estimate
  - Cost of Global Identity Theft to FIs: $222 billion
    - World Bank estimate
  - Cost of Cross Border Trade paperwork: $460bn
    - UN UNESCO estimate

University Bank

What do we plan to build? (1)

- A network hub
- TCP/IP peer to peer secure bank centric email payment messaging system
  - Transmit Payment instructions + Data
  - Secure Email incorporating privacy enabling technology
  - Data enabled for:
    - Micro-payments for Spam Blocking & Digital Content
    - Business 2 Business Payments/Invoice & Remittance Detail
    - Forex transaction engine for cross border transactions
    - *n* Web Services (e.g. sell to smaller FIs, geo-location)
- Secure Encrypted Database
  - Granular protection of data based on authorities and identities
  - Reduce Identity & Data Theft, Enhance Privacy
  - Theoretically infinite scalability of database
  - Global data accessible via web services
  - Lower cost of database operation & ease of maintenance
  - Easier disaster recovery/containment of security breaches
  - No matter WHERE the data went in the internet cloud, the data would still be protected and in order to access it, you would need to be strongly authenticated and authorized to do so.

University Bank

Cost of email Spam: $200 billion

- First Class Email
  - Strong Authentication + Federated Identity Management
  - Efficient email based secure micro-payment system
    - Extra marginal transaction is close to zero cost
    - Under 1/100th of a cent cost per completed transaction
- Eliminate 100% of noxious email spam for opt-in users
  - Eliminate viruses & email phishing
  - Spammers must pay at least $0.01 per email
- Spam blocking pays for the creation of the whole First Class Email hub
  - Build the network for one purpose – the beachhead
  - Roll out all the other services at a very low marginal cost

University Bank

First Class Emails: Consumers

- Dramatic reduction of time-wasting and annoying spam, viruses and phishing attacks
- Consumers are paid for the spam they actually receive
- Consumers can set the minimum payment amount at their desired level
  - Set minimum of $0.01 or optional higher amount (e.g. $1, $10, $500)
- No cost to the consumer, in fact they will make money over time from marketers who continue to annoy them
- Ease of use
- Ease of sign-up
- Can still send emails to non-adopters
- Consumers inherently trust their banks and hence it is a natural sale
  - Who would trust their bank account to a tech company???

University Bank

First Class Email: Consumers (2)

- Consumers will receive more money than they pay out
  - They will put cash in their pocket every day, week & month
  - The average consumer would gain $1 to $5 per month in net revenue from "First Class" email solicitations they receive in excess of email postage they pay out
  - The cost of their ISP service will drop (see below)
  - Additional web services will be available to them as a result: digital content, information services sold for less than $1.00 or less than $0.01
  - It will be much easier for them to pay their bills and be paid
  - The level of Identity Theft will drop sharply
  - Their confidence in their banks will rise sharply

University Bank

First Class Email: Direct Marketers

- Three things happen with First Class Email:
  - Consumer cashes the eCheck for $0.01 – put them on the Do Not Solicit List – valuable info
  - Consumer buys - $0.01 was a great investment
  - Consumer neither cashes the eCheck nor buys
    - This is very valuable info
    - Something about the offer was intriguing but either the timing wasn't right or they need more info to evaluate the offer
    - Hit them with additional product info
    - Send them direct mail, discount coupon with expiration date, telemarketing call & etc.
- Very valuable tool that allows Direct Marketers to become more targeted and efficient

First Class Email: Corporates

- Loss of productivity per employee linked to email is $300 per year
  - Tight filters cost sales
  - Loose filters cost productivity
- NAM: Loss to U.S. manufacturing industry is $9 billion per year
  - DaimlerChrysler: Annual cost of Global email is $300 million per year but well over half of network traffic is spam
    - T-1 lines, T-3 lines, servers, filtering, SANs, virus protection, network security issues
    - Potential cost savings is $150 million per year excluding productivity costs
- Get large corporates at the top of supply chains to adopt and the suppliers must follow
  - Lower costs and productivity gains per employee at $300 per employee, are:
    - $3,000,000 per year for a company with 10,000 employees
    - $30,000,000 per year for a company with 100,000 employees.
- Government agencies' economics are similar to large corporates

University Bank

First Class Email: ISPs

- Cost of email spam is approx. 30% of revenue base
  - Average profit is now 8% of sales
  - Decreased costs due to elimination of 80% or more of the network traffic that is spam prior to reaching their servers. The resources spent on connectivity can be reduced
  - Decreased costs due to elimination of viruses, worms and phishing attacks on customers. Substantial resources must currently be expended for security and customer service that will decrease
  - Increased customer satisfaction resulting in lower churn and higher retention
  - Increased profitability per customer
  - Opportunity to dramatically increase profit OR
  - Lower cost of service to consumers, further increasing internet penetration
- Who loses?
  - Limited few ISPs who cater to spammers will lose out
  - Limited few telcos who make money moving spam will lose out
- FTC is supportive of our proposal, as is the Commerce Department

First Class Email: Banks

- The banks that participate in the network will benefit by making additional profits with little risk.
- Each clearing bank acting as a correspondent bank would have a new business with a value of between $780 million and $1.30 billion at the end of the third year after product launch.
  - Correspondent banks would increase the value of each customer in the network by approximately **$180** assuming increased gross revenue of $18 per year, cost of service of $6 per year per customer and a multiplier on pre-tax profit of 15x.
- Banks earn greater loyalty and closer relationship with customers;

University Bank

First Class Email: Banks (2)

- Banks can earn money by providing additional identity management services beyond the actual email spam blocking service described here. If all customers were strongly authenticated additional web services could be sold on a fee for service basis.
- Banks have lower costs of serving consumers due to lower fraud losses and lower IT administrative costs due to a reduction in malicious viruses, Trojans and phishing attacks.

University Bank

Challenges of implementation

Phase 1 (analysis): FSTC Counter-Phishing Project ✓

Need for:

Phase 2 (testing & proof of concept):

- Consortia of large banks to announce test
- Testing:
  - Scalability
  - Feasibility
  - Usability

Phase 3 (launch):

- Announce Day 0 launch date 6-9 months out
- Advance sign-up utility
- Two large corporate early adopters at the top of a large supply chain
- At least three large banks
- At least one government agency

University Bank

Next Steps

- Proof of Concept
  - Committed
    - Leading IT Firm as integrator
    - University Bank
    - Jove Corporation/Internet Money Corporation
  - Discussions underway:
    - Major ISPs
    - Major banking industry payment networks
    - Top 5 U.S. banks
- Commitment from global FIs:
  - Agree to use the system if "Leading IT Firm" builds it
- Commitment from U.S. Gov't:
  - Agree to a system pilot if "Leading IT Firm" builds it
  - Significant agency productivity and cost savings from adoption of First Class Email
  - Significant military & intelligence implications of First Class Email

University Bank

What does each bank get?

- Option to buy 1 of the 10 global master licenses
  - $1.1 billion value +- $200 million by end of Year 3
  - Sell services to corporates and consumers
  - Resell services to smaller FIs
- Great PR on doing something about solving the email spam problem
  - Increased customer loyalty and customer satisfaction
- An opportunity to buy into Jove or *i*MC
  - Publicly traded and non-publicly traded investment option
- Side benefits
  - Strengthens the business model for other IT initiatives
  - Places banks in a leading position to sell additional web services for its Silicon Valley customer base
  - Allows banks to assist the entertainment industry to sell digital content cost effectively without risk of piracy

University Bank

Cost of Cross Border Trade paperwork: $460 billion

- Each invoice now costs $6 on average
  - 20% of domestic invoices require rework
  - 1 car moved from Mexico plant to Jacksonville car dealership requires 19 different invoices
  - Int'l invoices are more expensive
    - 90% of cross border invoices require rework
- XML and TCP/IP enabled Invoices would cost $1 plus $1 fee to banks (Fed'l Reserve Data estimate).
- Business saves $4 per invoice
  - With 100% penetration:
    - Annual savings $350 billion (estimate)
    - Banks increase revenues by $55 billion (estimate)
  - With 1% penetration:
    - Annual savings $3.5 billion (estimate)
    - Banks increase revenues by $550 million (estimate)

University Bank

Banking as Critical Infrastructure

- Pre 9/11
  - Need to synchronize the physical and financial supply chains for business savings
- Post 9/11
  - Need to synchronize the physical and financial supply chains for homeland security
  - With Sarbanes/Oxley and new customs requirements for Container Security, the risks, fines, and liabilities need to be understood and the nature and costs associated with legal compliance need to be assessed.
  - The business savings available can pay for a lot of security
    - $4 per invoice savings possible ($6 -> $1 + $1 fee for banks) (Fed'l Reserve Chicago 2004 Payments Conference estimate)
    - $460 billion per year in cross-border trade paperwork costs (UNESCO estimate) with $340 billion in total possible savings

University Bank

What are the outcomes?

- Investment in the First Class Email hub (*i*MC) will be worth:
  - $940mm to $1.550 billion
    - Assuming 10% market share of the 665mm email users globally at the end of three years
- First working prototype of Secure Encrypted Database
  - Built on "Leading IT Firm " hardware & software
  - Huge market potential from SED due to:
    - Lower cost of database operation & ease of maintenance
    - Theoretically infinite scalability of database
    - Granular protection of data based on authorities and identities
    - Easier disaster recovery/containment of security breaches
    - First mass market adoption driver to IPv6
- First true internet based payment system

University Bank

What could you do with a true Internet based payment system?

- Interoperability to all global bank legacy systems
- Move money with the ERP data globally
- Secure Encrypted Database Storage Area Network
  - Serve up data on demand via web service
  - Persistently secure data & digital content no matter where it goes in the future across the internet
- Real-time settlement with legal finality
- Global 24-hour rolling cash concentration
- Secure Trusted Messaging down to the customer level
  - TCP/IP and email based – 665 million global users
  - Eliminate email spam, email phishing, viruses & etc.
- Real-time re-work, manage the transaction at any point
- Synchronize the physical supply chain to the financial supply chain
- Role of banks: Leverage the Trust Relationship to provide Federated Identity Management, Risk Management, Risk Mitigation and Assurance of Payment
- BUT, costly, where to start? Where is the beachhead?

Businesses must meet Government mandates: Compliance Issues

- Government regulation will increase post Enron/9-11
  - The Risk related to new regulations is personal
    - E.g. Sarbanes-Oxley, Customs' 24-Hour Rule
  - Risk for identity management is real (e.g. Travel Rule)
  - Government mandates are expensive
    - Dirty data risky / info must be more real-time
  - Cost of logistics risk mitigation due to terrorism
- There is no way for business to comply without synchronizing the physical supply chain to the financial supply chain
  - ***The reduction in invoice & remittance costs pays for a lot of compliance & Homeland Security***
- Risk of new stronger mandates from government without action
- Great opportunity but hugely complicated:
  - Long sales cycle
  - No one person has global view that the company is drowning in rework and reconciliation
  - Where is the beachhead?

University Bank

CSI Status

Logistics Effects

Cargo

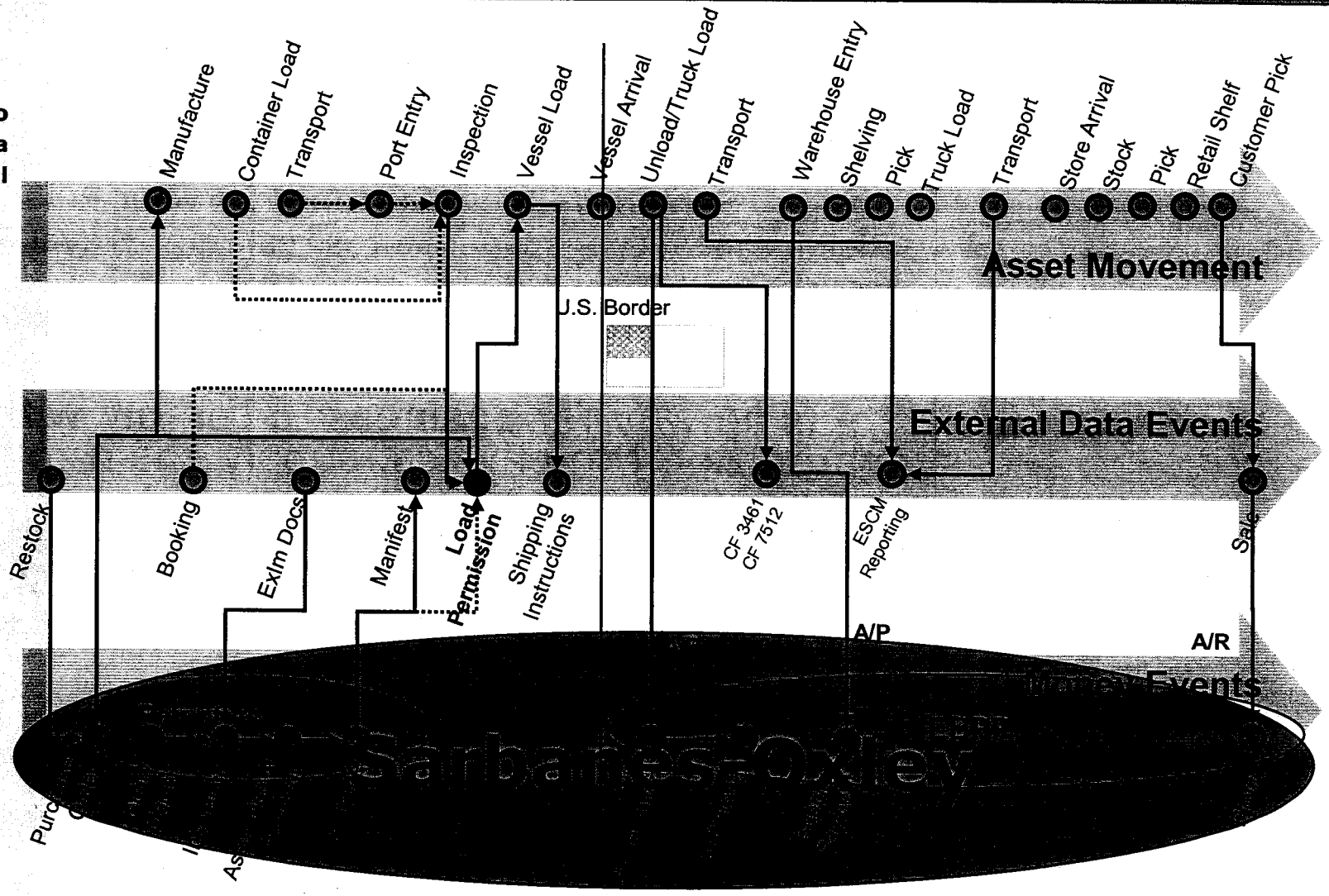
Data

Financial

Commoditization

Solution

Leadership Opportunities



Source: Covansys © 2003