

Data Security, Consumer Privacy and Identity Theft

MBA Legal Issues, San Diego, CA

Nov. 29, 2007



1. Legislation, Regulation and Advocacy
 - Government & Legal Affairs
2. MBA Technology Steering Committee
 - Board of Directors Technology Steering Committee (BoDTech)
 - Residential Technology Steering Committee (ResTech)
 - Strong Authentication White paper
3. Education
 - CampusMBA Five-Step Information Assurance Model
4. MISMO www.mismo.org
 - Information Security Work Group
 - Remote Authentication White paper
5. Identity Management
 - Secure Identity Services Accreditation Corporation (www.sisac.org)
 - Public Key Infrastructure (PKI) best practices policy

- Over 9,300,000 victims of ID theft in America
- 215,990,450 individual person record breached
 - FIs, retail, healthcare, education, Gov.
- \$182/record & \$4.8 million/incident
 - A 2007 survey by Ponemon Institute
- Forrester Research
 - Cost between \$90 and \$305 per lost record
- FBI - Mortgage fraud 4th highest crime category
- Over 35 states have Breach notification legislations
- TJX 94M credit and debit card account numbers potentially breached
 - \$100 per lost record, or a total of \$4.5 Billion
 - Pending liability with card issuers

Issues



- Cisco Report
 - 73% put security on IT
 - 44% open email/attachments from unknown
- Gartner Report
 - Over 70% of security vulnerabilities exist at the application layer, not the network or system layer
 - NIST claims this number of 92%
- CERT E-Crime Watch Survey
 - 12% increase in insider Identity Theft
- A critical security breach that exposed nuclear secrets at the Los Alamos Labs was the result of human error and not security processes

Dangerous Technologies



- ❖ Instant Messaging
- ❖ Web mail
- ❖ Portable Storage devices
- ❖ PDAs
- ❖ Smart/Camera Phones
- ❖ Voice-over-IP
- ❖ Social networking
- ❖ Wiki

Introduction to Authentication



- Definition
 - The process used to confirm an individual's identity as a party in a transaction.
- Used in two contexts:
 - When relationship between the parties is first created
 - When a Transaction occurs in the course of an existing relationship.

Why is Authentication Important?



- Assists in compliance with applicable laws
- Promotes legal enforceability of electronic agreements and transactions
- Builds consumers' trust in electronic agreements and transactions
- Mitigate risk of threats & vulnerabilities
 - Reduce identity theft

- The agencies consider single-factor authentication, as the only control mechanism, to be inadequate for *high-risk* transactions involving access to customer information or the movement of funds to other parties.
- Account fraud and identity theft are frequently the result of single-factor (e.g., ID/password) authentication exploitation.
- *High Risk Transactions*
 - Finance transfer
 - Transfer of Personal Information

Solution



- ❖ Factors are usually based on:
 - ❖ Something you have; password, PIN
 - ❖ Something you know; Token, Digital Certificate
 - ❖ Something you are; biometrics

- ❖ Solutions
 - ❖ Shared Secrets and Images
 - ❖ Cookies
 - ❖ Tokens
 - ❖ Keystroke recognition
 - ❖ Digital Certificate

Implementation



- Verified by Visa
 - Splash box that requires password/PIN for retail credit card transactions
- eTrade
 - One-time-password tokens
 - A 6-digit random number that changes every minute
- Bank of America
 - SiteKey - Customer selects a small image and a brief phrase - and then select three challenge questions. This information is then requested whenever the customer logs in to access an online account.

- HTTP Cookies
 - Cookies are something a person has and are loaded onto a user browser by the web server.
 - Cookies contain authenticating (user ID and password), tracking (shopping cart), or specific information.
 - End users have no interaction with cookies.
 - Authentication Cookies should be *encrypted* and coupled with another authentication factor such as a shared secret.
 - Initial pre-screening process prior to loading cookie
 - General wallet or account information (something they know)
 - Backup process
 - Customers don't always use the same computer
 - Secondary authentication method (similar to initial screen process)
- Good migration strategic to stronger authentication

National Notary Assoc (NNA)



• Requirements

- Provide national background screening service for title, settlement services, lenders

• Screenings

- Lexis/Nexis, Sungard/Signix
- County-level criminal records check
- SSN name check
- OFAC
- Other screening criteria
- Matrix score results in pass/fail
- Appeals process and resolution

MERS –eNote Registry



- Designation of authoritative Promissory eNote
- Single source for Mortgage Industry of electronic Note
 - Notes are traded between primary, warehouse, secondary.
- Launch production
 - April 26, 2004
- MERS Requirements
 - Tamper-evidence seal on envelope
 - SISAC Organizational Medium Assurance Cert
 - Individual Identity on specific Transactions
 - SISAC Individual Medium Assurance Cert

Secure Identity Services Accreditation Corporation



SISAC

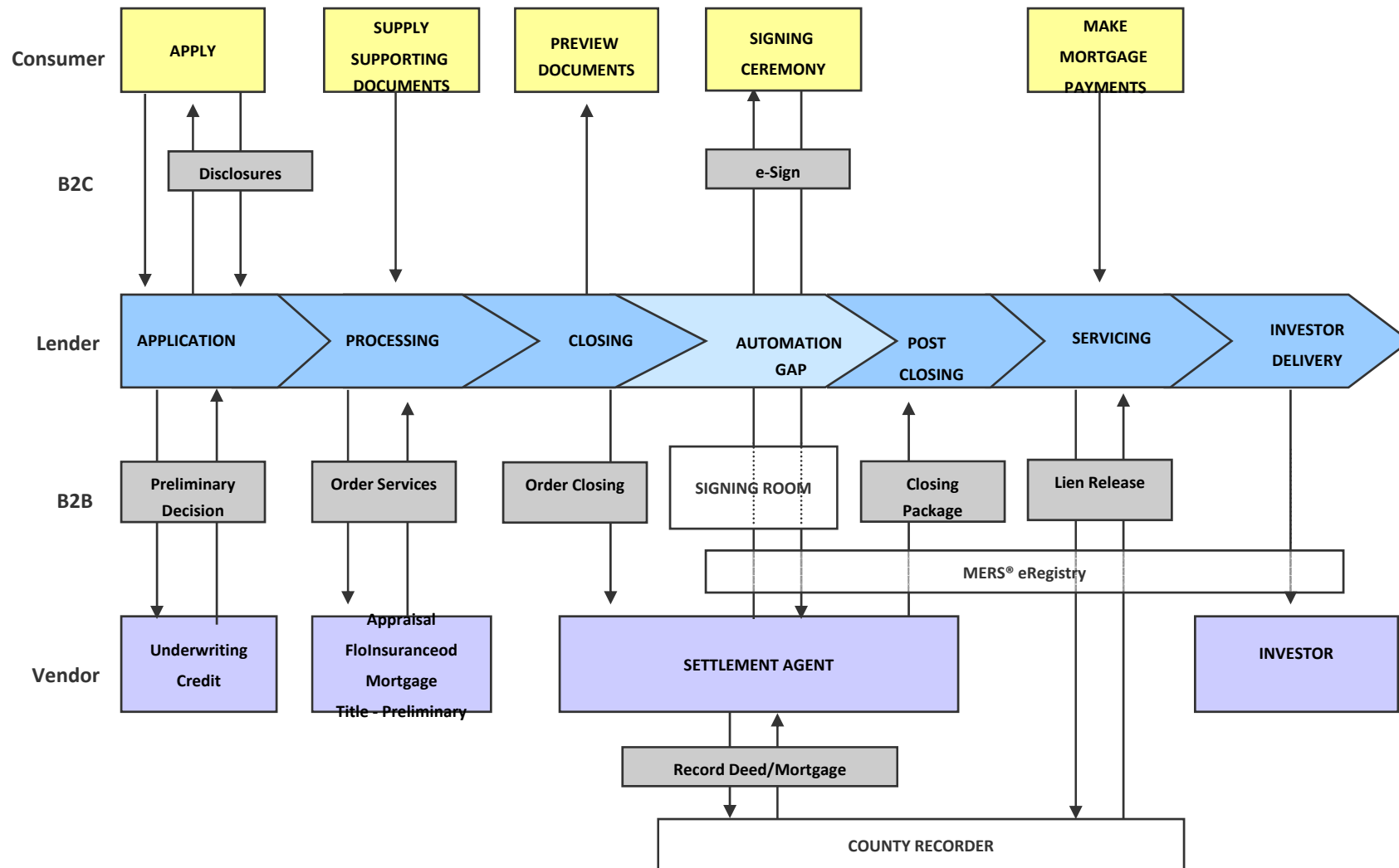
- Develops baseline standards for auditing and accreditation of certificate/credential issuers
 - SISAC does not issue credentials, rather accredits Service Providers, e.g., VeriSign, GeoTrust, etc.
- Technical, Business and Legal requirements
- B2B model for authentication
- Wholly-owned subsidiary of MBA
- www.sisac.org

Assurance Levels



	Subscriber		
	Type 1 (Basic)	Type 2 (Medium)	Type 3 (High)
I&A Reqs.	Name, address, telephone #, e-mail address, Social Security number, state-issued photo identification card number, or shared secret.	In-person proofing. Credentials required are either one Government-issued Picture I.D.; or two Non-Government IDs.	In-person proofing. Credentials required are either one Government-issued Picture I.D.; or two Non-Government I.Ds.
Activation Data	Initial Activation: User selected (PIN, phrase, etc.) Subsequent Activation: Single factor (e.g., password)	Initial Activation: User selected (PIN, phrase, etc.) Subsequent Activation: Single factor (e.g., password)	Initial Activation: Out of band & acknowledgment Subsequent Activation: Two factor (i.e., possession of hardware token and known secret (e.g., PIN) to access token)
Private Key Storage Reqs.	None (Software)	FIPS 140-2 Level 1 (Software or Hardware)	FIPS 140-2 Level 2 (Hardware)
Insurance Reqs.	\$1M aggregate	\$5M aggregate	\$10M aggregate
Revocation Notification	Within 24 hours	Within 12 hours	Within 6 hours

eMortgage Process Flow



Thank you!

R. J. Schlecht

Director, Industry Technology Security and Compliance

(202) 557-2843

rschlecht@mortgagebankers.org