Game Theory Assumptions

- **Knowledge assumption**
  - Parties know outcome values

- **Causative assumption**
  - Game outcomes drive choice

- **Bilateral game assumption**
  - Only 2 parties involved in game
  - No spillover effects

- **Binary choice assumption**
  - Choice is cooperate or not
  - No other alternatives
Knowledge Assumption

• Game theory assumes players know outcome values.

• Static model, but dynamic world in which outcomes change.

• Immediate costs vs. unclear benefit.
Causative Assumption

• Game theory assumes that players act based on expected game outcomes.
  – Usually this is expressed as a rationality assumption.

• But security is not a stand-alone product.
  – Part of a bundle of features in a payment system.
  – FIs, Merchants, and Consumers choose rationally, but based on total bundle of features.
  – There isn’t a “security” game.
Bilateral Game Assumption

• Game theory usually models 2-player games.
  – Multi-player models are harder to model.
    • Stable Nash equilibrium is guaranteed possible if no coalitions
  – But payments security is often a multi-player game.

• Game theory does not model third-party externalities (spillover costs/benefits to non-players).
  – E.g., data breach at merchant 1 results in fraud losses for merchant 2, 3, & 4 and at banks X, Y, and Z.
Binary Choice Assumption

• Game theory often assumes a binary choice: cooperate or not.

• But real life is not binary choice.
  – Alternative to cooperating in game 1 is to cooperate in game 2, 3, 4, etc.
  – Much harder to model universe with multiple simultaneous games (additivity problem).
Implications of Game Theoretic Limits

• Knowledge assumption
  – Need for data

• Causative assumption
  – Need for competitive markets to achieve efficient outcome.

• Bilateral game assumption
  – Need for fair markets (no uncompensated spillover effects)

• Binary choice assumption
  – Need for competitive markets to achieve efficient outcome.
Key Payments Security Policy Goals

1. Data
   - Helps achieve efficient outcomes.
   - Facilitates primary actors’ choices
   - Facilitates secondary risk markets

2. Competitive markets
   - Ensures payments security rules are set based on security outcomes, not other considerations, like growth.

3. Fairness
   - Prevent or mitigate negative spillover effects.
How to Achieve Payment Security Policy Goals?

• Three major approaches are currently used.
  – Private ordering (contract)
  – “Hard” regulation (rulemaking)
  – “Soft” regulation (nudges & policing)

• Different approaches appear in different contexts.
  – Security rules
  – Fraud loss prevention/mitigation rules
  – Fraud loss allocation rules
“Soft” Public Ordering

• Convening/coordination role
  – Government as neutral convener (FPTF, SPTF, MPIW)

• Data collection
  – Enables empirical research
  – Enables secondary and insurance markets
  – Definitional and standard-setting function

• Regulatory “guidance”
  – Formally non-binding regulatory instruction
  – But functionally followed

• Antitrust enforcement
  – Case specific, but improves private ordering overall

• Provision of “public options” that frame competition.
  – Fed’s role as operator for ACH and check clearing
Security Rules

• Set by private contract only.
  – Single-system rules (network rules)
  – Collaborative standards (e.g., PCI)

• But AML, national security, and reputational concerns lurk.
  – “Soft” regulatory pressures
Fraud Loss Prevention & Mitigation Rules

- LP&M rules are set by command & control public law.
  - State data breach notification laws.

- LP&M rules also function as a type of loss allocation rule, in that they impose costly duties on certain parties.
  - Unclear if costs outweigh losses averted.
  - If costs > losses averted, then LP&M rules function as a penalty.
Fraud Loss Allocation Rules

• Fraud loss allocation rules shape incentives for adopting security rules.

• Fraud loss allocation rules are set in part by private contract and in part by public law.
  – Private ordering (contract)
    • Network rules for credit, debit, ACH
    • Bilateral checking rule arrangements
  – Public law (“hard” regulation)
    • Checking system (UCC Art. 4)
    • Consumer liability rules for all systems
Consumer Unauthorized Transaction Liability Rules

- Consumer liability rules combine public law and private ordering.
  - Public law
    - TILA/Reg Z; EFTA/Reg E; UCC Article 4
  - Private ordering
    - Various network rules (incl. zero liability policies)

- Consumer liability rules are inconsistent across systems.
  - Some systems have capped strict liability or contributory negligence liability.

- Generally, however, consumers have little or no liability for unauthorized transactions.
  - Protects players with the least market power.
# Inconsistent Consumer Liability Rules

<table>
<thead>
<tr>
<th>System</th>
<th>Law</th>
<th>Consumer Liability for Unauthorized Transaction</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Credit</strong></td>
<td>TILA/Reg Z</td>
<td>Strict liability, but capped at $50.</td>
</tr>
<tr>
<td><strong>Debit</strong></td>
<td>EFTA/Reg E</td>
<td>Strict liability, but capped at $50, unless consumer was negligent, then $500 or unlimited.</td>
</tr>
<tr>
<td><strong>ACH</strong></td>
<td>EFTA/Reg E + NACHA Rules</td>
<td>No consumer liability.</td>
</tr>
<tr>
<td><strong>Checks</strong></td>
<td>UCC Art. 4</td>
<td>No liability unless negligent.</td>
</tr>
<tr>
<td><strong>Cash</strong></td>
<td>Common law</td>
<td>Unlimited liability.</td>
</tr>
</tbody>
</table>
Unintended Consequences of “Hard” Regulation

• Often, faster payments = less secure payments
  – e.g., single-factor authentication; unencrypted data.

• Some merchants want faster payments to increase sales.

• Consumers are willing to use less secure payment methods because they do not usually bear fraud losses.

• Full costs of faster, less secure payments are not internalized by merchants who use them.
  – Security lapse at one merchant can cause losses for other merchants and banks.
  – Conditions consumers to expect faster/easier payments; harder for slower systems to compete.
Imperfect Solutions

• Solution 1: Increase consumer unauthorized transaction liability for less-safe systems.
  – Incentivizes consumers to demand safety.
  – But works only if consumers end up actually liable.
    • Not worthwhile for small dollar transactions
    • Network zero liability policies force subsidization of consumers by banks & merchants.
  – Doesn’t fully internalize spillovers.
  – Politically difficult.

• Solution 2: Minimum mandatory standards across systems.
  – E.g., mandatory two-factor authentication or encryption.
  – Prevents uncompensated externalities.
  – Cf. minimum product safety or environmental regulations.
  – But what should these standards be? How detailed?
  – And who should set them?
## Private vs. Public Tradeoffs

<table>
<thead>
<tr>
<th></th>
<th>Private Ordering</th>
<th>Public Ordering</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsive?</td>
<td>More</td>
<td>Less</td>
</tr>
<tr>
<td>Expertise?</td>
<td>More</td>
<td>Less</td>
</tr>
<tr>
<td>Accounts for Externalities?</td>
<td>No</td>
<td>Potentially</td>
</tr>
<tr>
<td>Transparent &amp; Open Process?</td>
<td>Less</td>
<td>More</td>
</tr>
<tr>
<td>Other Influences?</td>
<td>Market power</td>
<td>Politics</td>
</tr>
</tbody>
</table>
Payment Security Policy Agenda

• **Data Collection**
  – Need data collection in standardized forms
  – Enables market discipline in primary markets
  – Facilitates secondary risk markets (insurance, derivatives, securitization)
  – Enables better policy making

• **Antitrust**
  – Socially optimal security choices require competitive markets.
    • But natural monopoly problem because of network effects
    • Mobile ecosystem exacerbates competition problems.
  – Antitrust enforcement is an imperfect policy tool.

• **Reduce Externalities**
  – Mandatory liability rules to incentivize care and reduce spillovers?
  – Minimum mandatory standards to reduce spillover effects?
  – Risks of intended consequences.