Automation and Disruption in Stolen Payment Card Markets

Timothy Peacock
Shape Security

Allan Friedman
George Washington University
Payments System Model

Card Network

Acquiring Bank

Merchant

Issuing Bank

Card Holder
Card Value Extraction Chain

Breach ➔ Wholesale ➔ Retail/ Card shops ➔ Cashout
Refining

Set of small-value, large volume websites.

Pool of stolen payment cards

Unsuccessful transactions

Successful transactions

Known good cards
To be sold
Existing Real-Time Anti-Fraud

- Find horse hoofprints
- Detect, then remediate
- Retrospective, not preventative
Proposed Intervention

● Stop automated payment card use

● Value chain choke-point

● Technology agnostic
# Refining vs. Cashout Merchants

<table>
<thead>
<tr>
<th>Refining</th>
<th>Cashout</th>
</tr>
</thead>
<tbody>
<tr>
<td>Large transaction volume website</td>
<td>High value transactions</td>
</tr>
<tr>
<td>Low value per transaction</td>
<td>Fungible, resellable goods</td>
</tr>
<tr>
<td>Low impact from fraud</td>
<td>Larger pain from fraud</td>
</tr>
<tr>
<td>Enable downstream harms</td>
<td>Cannot see upstream enablers</td>
</tr>
</tbody>
</table>
How Do We Get There

- Regulatory
- Liability
- Cross-subsidy
Implications

- Chip+PIN
- Acrimonious lobby fight
- Small intervention: big change
Limitations, Future Work

- Quantifying impact
- Empirical grounding