Data Distribution Security for 2018 and Beyond

Tools and policies to help distribute real estate data securely.

RESO Fall Conference
October 17, 2018
Historically data security was "built in"

Data Distribution in the 70’s, 80’s and yes even the 90’s

Welcome to the 90’s, the start of listing data on the Internet
MLSs and Brokerages are evaluating their risk
As a result, they are demanding more

**RISK CHALLENGES**

- Privacy legislation and breach notification
- Wire fraud and business email disruption
- Consumer "trust" must be maintained
- Demand for property data at an all time high

**MITIGATION STRATEGIES**

- Tighter vendor/partner screenings for security and business continuity
- Tighter internal access controls (2FA and more)
- Data governance process for all data stored and/or licensed
- Limit data distribution to only what is "necessary"
Security is critical
BUT, so is balance
Speaking of convenience

RESO Best Practice - Secure, convenient standard for SSO

- User has SSO from single login across disparate systems
- User can self-link the accounts
- System owners can set linking policies that meet their business and security needs
- Built on open standards
## Data Distribution Security

### Top “Difference Makers”

<table>
<thead>
<tr>
<th>MLS</th>
<th>Broker</th>
<th>3rd Party Recipient</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data license associated with every authorized feed</td>
<td>Know where your data is going and what tools get it there</td>
<td>Deploy and properly manage intrusion detection tools</td>
</tr>
<tr>
<td>Get specific in license agreements including “only the data needed” and “reasonable care”</td>
<td>Ensure all software you use has licensed the rights to the data that powers it</td>
<td>Anti-scraping and bot detection tools are now a minimum “standard of care”</td>
</tr>
<tr>
<td>Strong credential management, including forced changes and strong PWs</td>
<td>Monitor and control access to data that includes PII and/or PSI for both agents and consumers</td>
<td>Absolutely no derivative works if the license agreement doesn’t specifically allow it</td>
</tr>
<tr>
<td>Appropriate copyrights in place</td>
<td>Deploy anti-scraping tools on your public facing website</td>
<td>Routine security audits by external 3rd party</td>
</tr>
<tr>
<td>Usage monitoring for abnormal or unauthorized activity</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Introducing Trestle Defender
Comprehensive protection for participating clients

### Data Security Diagnostic & Protection Kit
- Assess customer risk and provide tools and reporting to identify bad behavior.
  1. Data Distribution RISK assessment
  2. Best Practices review
  3. Enhanced password management
  4. Data usage reporting

### Secure Distribution via Trestle
- Secure distribution of data and compliance with licensed use.
  1. Data distributed only to licensed recipients
  2. Risk detection, scoring, reporting and alerts for fraudulent activity and overuse
  3. Remediation actions for fraudulent activity
  4. Data seeding

### Real Estate Data Intelligence Sharing Tool
- Contributory database of high risk data users.
  1. Fraud risk scores above a certain threshold included
  2. Simple process to report potential violators
  3. Dashboard for Trestle customers to view fraud risk scores across customers base.
Why Trestle Defender?
More protection for your most valuable asset

- Protects data assets the way SAFEMLS protects the MLS system “front door”
- Lowers compliance cost for MLS by providing intelligence and automated remediation
- Guides enforcement of terms of use and other MLS data licensing requirements.
- Demonstrates continued commitment to security and protection of your data
Thank You!

Amy Gorce
CoreLogic
amgorce@corelogic.com