Brand Protection Needs in the Pharmaceutical Industry

The Global Problem of Counterfeit Pharmaceuticals
Assessing Risks As Part of a Brand Protection Program

University of New Hampshire
School of Law

David S. Howard
Industry Fellow
Michigan State University
February 20, 2014
Building for Success – Basic Principals in Brand Protection

- Prosecution and Enforcement
- Detection
- Authentication
- Process Control
Authentication – What Makes This One True and Originally Ours???
Track and Trace - Where Is The Product Headed, Where’s It Been, Where Is It Now?

- Prosecution and Enforcement
- Detection
- Process Control
- Authentication
You Cannot Prosecute What You Cannot Find, So You Must Detect.
Making Use of Your Findings, Making It Hurt, Making It Stick, Making It Public…

- Prosecution and Enforcement
- Detection
- Authentication
- Process Control
Holistic Approach To Brand Protection

- Prosecution and Enforcement
- Detection
- Authentication
- Process Control
Holistic Approach To Brand Protection

Understanding Risks

- Authentication
- Detection
- Process Control
- Prosecution and Enforcement
Assessing Product Risk

Spreading the “Big Six” thinking
R&D Understanding and Integration
Product and packaging considered
Manufacturing and Packaging locations reviewed
Distribution locations and processes reviewed
Pricing strategies feeding diversion trends
Logistics strategies feeding counterfeiting trends
Company practices feeding both
The Big Six Questions…

1) To your knowledge, has this product class or brand ever been counterfeited?
2) To your knowledge, has this product class or brand ever been illegally diverted?
3) Have you ever looked for counterfeit or diverted product in the marketplace?
4) Have you ever investigated the return goods process to determine the type and flow of products being returned?
5) Have you ever investigated the product complaint history process to determine if product tampering or diversion may be misreported as miscellaneous complaints?
6) Have you ever investigated the product and packaging destruction process to determine adequacy and thoroughness of product destruction?
The Remaining Questions…

There are additional questions used to drill down to the potential sources of and insights into product, market, and regional factors that can lead to increased ease in counterfeiting and illegal diversion of products.

A team effort is needed to understand how products are developed, marketed, distributed, repackaged, reprocessed, dispensed, consumed and disposed.

Requires looking upstream and downstream, from sourcing through manufacturing, in distribution through your chosen channels.

Requires understand this level of detail globally, not just domestically.
A-CAPP Paper Series

Assessing the Risks of Counterfeiting and Illicit Diversion for Health Care Products

Christopher Trent
Senior Manager
Product Protection
Johnson & Johnson Global Brand Protection

Douglas C. Moyer, Ph.D., CPP
Adjunct Instructor
Program in Public Health
Michigan State University

November 2013
For More Information on Risk Assessment Please Consider The Following

- [http://a-capp.msu.edu/sites/default/files/HealthCareProductsRisk_Trent_PaperSeries_FINAL.pdf](http://a-capp.msu.edu/sites/default/files/HealthCareProductsRisk_Trent_PaperSeries_FINAL.pdf)
If Risks Exist, Protect…

Product Protection is . . .

- Assessing the risk to each product
- Protecting products AND packaging
- Developing product protection standards
- Deployment of product protection features

Product Protection is not. . .

- Slapping features on products to solve unknown problems
- An inexpensive way to improve defects in packaging design
### Assessing Where You Are

<table>
<thead>
<tr>
<th>Secure Supply</th>
<th>Program Management</th>
<th>Monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>No features</strong></td>
<td><strong>Common Security Features</strong></td>
<td><strong>Common Security Features With Integrated Program Management</strong></td>
</tr>
<tr>
<td><strong>Security Features</strong></td>
<td><strong>Common Security Features With Supplier Program Management</strong></td>
<td><strong>Common Security Features</strong></td>
</tr>
<tr>
<td>• Proprietary feature deployed</td>
<td>• Standard proprietary feature deployed</td>
<td>• Standard proprietary feature deployed</td>
</tr>
<tr>
<td>• Little to no operating company oversight to manage the feature</td>
<td>• Little to no operating company oversight to manage the feature</td>
<td>• Management of the supply process by the Supplier</td>
</tr>
<tr>
<td>• Feature is not standard across the sector</td>
<td>• Feature is not standard across the sector</td>
<td>• No/informal monitoring</td>
</tr>
<tr>
<td>• No monitoring plan</td>
<td>• No monitoring plan</td>
<td>• Monitoring device available to authenticate product</td>
</tr>
<tr>
<td>• No formal integration into product design or bill of materials</td>
<td>• No formal integration into product design or bill of materials</td>
<td>• Formal integration into product design and bill of materials</td>
</tr>
<tr>
<td>• Monitoring device available to authenticate product</td>
<td>• Monitoring device available to authenticate product</td>
<td>• No/informal monitoring</td>
</tr>
</tbody>
</table>

- Commodity feature deployed OR
- Inconsistent application of the feature OR
- Monitoring device not available or not developed to enable authentication
## Determining How To Advance

<table>
<thead>
<tr>
<th>Secure Supply</th>
<th>Program Management</th>
<th>Monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>No features</strong></td>
<td><strong>Common Security Features</strong></td>
<td><strong>Common Security Features</strong></td>
</tr>
<tr>
<td></td>
<td><strong>With Supplier Program Mgmt</strong></td>
<td><strong>With Integrated Program Management and Effective Monitoring</strong></td>
</tr>
</tbody>
</table>

### No features
- Commodity feature deployed OR
- Inconsistent application of the feature OR
- Monitoring device not available or not developed to enable authentication

### Security Features
- Proprietary feature deployed
- Little to no operating company oversight to manage the feature
- Feature is not standard across the sector
- No monitoring plan
- No formal integration into product design or bill of materials
- Monitoring device available to authenticate product

### Common Security Features
- Standard proprietary feature deployed
- Little to no operating company oversight to manage the feature
- No monitoring plan
- No formal integration into product design or bill of materials
- Monitoring device available to authenticate product

### Common Security Features With Supplier Program Mgmt
- Standard proprietary feature deployed
- Management of the supply process by the Supplier
- No/informal monitoring
- Monitoring device available to authenticate product

### Common Security Features With Integrated Program Mgmt
- Standard proprietary feature deployed
- Management of the supply process by the Supplier and OpCo
- Formal integration into product design and bill of materials
- No/informal monitoring
- Monitoring device available to authenticate product

### Monitor
- Standard proprietary feature deployed
- Management of the supply process by the Supplier and OpCo
- Formal integration into product design and bill of materials
- Formal monitoring program identified and resourced
- Formal training kits created for monitoring programs
How To Move Forward

Secure Supply

- No features
- Security Features
- Common Security Features
- Security Features With Program Mgmt.

Program Management

- Security Features With Program Mgmt.
- Common Security Features With Program Mgmt.
- Common Security Features With Protection And Effective Monitoring

Monitor

- Common Security Features With Protection And Effective Monitoring
- Interject program management
- Interject program management
- Interject program management

- Implement the standard security feature used across the sector
- Implement from Known Authentication Providers
- Monitoring forecasts and utilization of the feature
- Monitoring forecasts and utilization of the feature

- Evaluate options for features
- Review product Supply Chain specifics
- Develop an effective feature for monitoring
- Ensure ability to monitor throughout the supply chain
- Reliable Source of Authentication from RFI
- Identify and resource formal monitoring program
- Create formal training kits for monitoring programs (returned goods, customs, and field monitoring)
Thoughts On Technology…

• Know what problem you are trying to solve first.
• Get as close to the product as you can do so affordably.
• No single technology can assure a product will not be counterfeited.
• Layers must be utilized and features must be changed, stay nimble.
• No technology should be deployed without a plan for monitoring it in the field, ever.
• No technology should be deployed that cannot be updated in a moments notice.
Incident Management

- Every new incident should be measured against the Product Risk Assessment Questionnaire
- Questions should be updated if they are found to be inadequate or incapable of detecting counterfeit, diversion, or tampering risks.
- Annual review of questions a must
- Never stop updating and improving
Holistic Approach To Brand Protection

- Understanding Risks
- Authentication
- Detection
- Process Control
- Prosecution and Enforcement
Brand Protection Needs in the Pharmaceutical Industry

The Global Problem of Counterfeit Pharmaceuticals
Assessing Risks As Part of a Brand Protection Program

Thank You
DavidSHoward@rcn.com
(610) 217-7158

David S. Howard
Industry Fellow
Michigan State University
February 20, 2014