

**The International Market
For
Brand Protection Solutions
For
Electronic Equipment & Components**

ICs, PCBs / PCAs, capacitors, transistors, resistors. Batteries & cables. Industrial switchgear, switches, relays. Consumer electronics. PCs and peripherals. Mobile phones & accessories. Household & personal care devices. Domestic entertainment equipment

April 2009

Authors: James Bevan & Jeremy Plimmer



Vandagraf International Limited
Croftta House, Groes Faen, Mid-Glamorgan CF72 8NE, United Kingdom
Tel +44 (0) 1443 231 441. Fax +44 (0) 1443 223 876
email: info@vandagraf.com
www.vandagraf.com

TABLE OF CONTENTS

Forward

Executive Summary

Background

Electronic Components

Batteries

Computer equipment, components and accessories

Mobile Telephones and accessories (excl. Batteries)

Other Electronic Equipment – An Overview of Other Product Types affected by Counterfeiting

Security Features and Brand Protection Systems – Labelling & Packaging Applications - Electronic Equipment & Components

Financial Losses

1. Overview – Electronic Equipment & Components

1.1 Table Security risks - Product related through the supply chain in Electronics Equipment & Components

1.2 Table Countermeasures – Appropriate to product related crime in Electronics Equipment & Components

1.3 Structural Shifts in the World Electronics Industry have been a Key Driver of Counterfeiting in the Sector

1.3.1 Regional Trends - Electronic parts and components.

1.3.2 OEM global strategies

1.3.3 Counterfeiting is a major problem in the Electronics Sector

1.3.4 Ways that Counterfeiters operate in the Electronics Sector

1.3.5 Geographical Trends in Counterfeiting of Electronics

1.3.6 The dynamics of Chinese counterfeiting operations - Electronic parts and components

1.3.7 Selling Counterfeit Electronic Goods by means of the Internet

1.3.8 The Next 10 Years – Trends in Global Manufacturing – Electronic Equipment and Components

2. Electronic Components

- 2.1 Market Overview – Electronic Components
- 2.2 Product Related Crime – Electronic Components
 - 2.2.1 Leading problem area for Counterfeit Electronic Components - Low cost, relatively simple 'generic' components
 - 2.2.2 Case Study – Counterfeit LM4051 Voltage References
 - 2.2.3 Case Study – Counterfeit Audio Power Transistors
 - 2.2.4 The Nature of IP Violation in the Electronic Components Business
 - 2.2.5 Types of IP Violation and Counterfeiting – Electronic Components
 - 2.2.6 Types of problems arising from IP Violations – Electronic Components
 - 2.2.7 ICs versus PCBs – Vulnerability to Counterfeiting
 - 2.2.8 Case Study – Counterfeit ICs (Integrated Circuits) – Some Recent Findings by Semiconductor Insights (SI)
 - 2.2.9 US Customs and Border Protection service seizures in 2008 and a joint operation with the European Union
 - 2.2.10 Counterfeit Electronics in the United Kingdom – A Summary of the Situation
 - 2.2.11 The US and the EU crack down on counterfeit electronic components
- 2.3 Brand Protection – Electronic Components
 - 2.3.1 Organisational and Management Steps towards assuring the security of their supply chains for electronic parts and components.
 - 2.3.2 Electronic Components - Product Packaging can help to mitigate overall Risk
 - 2.3.3 Printed Circuit Boards (PCBs) versus Integrated Circuits (ICs)
 - 2.3.4 Case Study - Security Labelling Requirements for Printed Circuit Boards (PCBs)
 - 2.3.5 Labelling requirements – Printed Circuit Boards (PCBs)
 - 2.3.6 RFID chips mounted on PCBs / PCAs – A Solution from Silica / Avnet Inc. that improves visibility in manufacturing and can also provide enhanced brand protection
 - 2.3.7 High performance self-adhesive tapes for assembling components in the electronics industry can incorporate security features - tesa-scribos
 - 2.3.8 Several organisations that are taking a pro-active and strong stance against this threat in the electronics sector

2.4 Opportunities for Brand Protection Solutions – Electronic Components

3. Batteries

3.1 Market Overview – Batteries

3.2 Product Related Crime – Batteries

3.2.1 Case Study – Deployment of the 'Kodak Traceless' System for Anti-counterfeiting on Kodak Li-Ion Rechargeable Digital Camera Batteries

3.2.2 Case Study - Counterfeit Nokia rechargeable batteries seized by Customs Officers in Hong Kong

3.2.3 Case Study - Batteries: One of the world's most consumed items – Significant problems with potentially dangerous, sub-standard counterfeit products

3.3 Brand Protection – Batteries

3.3.1 Case Study – Rechargeable batteries - Original Nokia Battery Labelling Program Latest Step in Fight against Unsafe Counterfeits

3.3.2 Case Study - Security Labels for a Motorola Mobile Telephone Rechargeable Batteries

3.3.3 Case Study – Rechargeable batteries - Sony Ericsson Use Hologram label

3.3.4 Case Study - Rechargeable battery pack from Sony carries an authentication hologram and a covert EAS tag on the clam shell blister pack

3.3.5 Case Study – An Integrated Circuit (IC) Based Cryptographic Battery Authentication Technology from Atmel

3.4 Opportunities for Brand Protection Solutions – Batteries

4. Computer equipment, components and accessories

4.1 Market Overview - Computer equipment, components and accessories

4.1.1 Case Study – Tamper Evident Features and RFID to Deter Pilfering of Carton Contents – Hewlett Packard Desktop Printers

4.2 Product Related Crime - Computer equipment, components and accessories

4.2.1 Case Study - **The seizure of £38 million UK pounds worth of counterfeit Cisco electronic equipment has raised concerns over the security of networks**

4.3 Brand Protection - Computer equipment, components and accessories

4.3.1 Case Study – Holographic Brand Protection Label - Microsoft Mouse

- 4.3.2 Case Study - 3Com introduces 3-Dimensional holographic label to 3Com switches to protect partners and end users from non-authentic 3Com switches
- 4.3.3 Case Study - 3m tamper evident package seal designed to protect PC computer components and to assure that they are genuine
- 4.3.4 Case Study – Brand Protection Security Label - Sony Vaio PC Laptop
- 4.4 Opportunities for Brand Protection Solutions - Computer equipment, components and accessories

5. Mobile Telephones and accessories (excl. Batteries)

- 5.1 Market Overview – Mobile Telephones and accessories (excl. Batteries)
- 5.2 Product Related Crime – Mobile Telephones and accessories (excl. Batteries)
 - 5.2.1 Case Study – Seizures of Mobile telephone accessories at US port in late 2008
 - 5.2.2 Case Study - More than 30% of all mobile telephone handset sales in Uganda are counterfeit
 - 5.2.3 Recent Trends in Counterfeit Mobile Telephone Handsets
 - 5.2.4 Counterfeiting of mobile telephone accessories
 - 5.2.5 Other types of product related crime – Tampering, Warranty abuse, Theft - Mobile telephones and accessories
- 5.3 Brand Protection – Mobile Telephones and accessories (excl. Batteries)
 - 5.3.1 Case Study – Nokia mobile telephone handset with a brand protection holographic security label
 - 5.3.2 Case Study – Injection moulded battery charger cable with integrated Motorola logo provide some defense against counterfeiting
 - 5.3.3 Case Study - An Integrated packaging solution provides enhanced brand protection – Nokia mobile telephone kit, including handset, rechargeable battery and accessories
- 5.4 Opportunities for Brand Protection Solutions - Mobile Telephones and accessories (excl. Batteries)

6. Other Electronic Equipment – An Overview of Other Product Types affected by Counterfeiting

- 6.1 Market Overview - Other Electronic / Electrical Product Types affected by Counterfeiting – An Overview

- 6.2 Product Related Crime - Other Electronic / Electrical Product Types affected by Counterfeiting – An Overview
 - 6.2.1 Case Study - UL Warns of Potentially Hazardous Counterfeit AC Adaptors
 - 6.2.2 Case Study - Counterfeit Electrical Lighting Products - UL Warns of Potentially Hazardous Fluorescent Portable Lamp
 - 6.2.3 Case Study – Some other examples of Counterfeit Electrical Lighting Products and related connecting cables and switches
 - 6.2.4 Case Study - Counterfeiting of Power Tools
 - 6.2.5 The tip of the iceberg – Counterfeiting in the Electronics sector

7. Security Features and Brand Protection Systems – Labelling & Packaging Applications - Electronic Equipment & Components

- 7.1 How authentication technologies can assist in the fight against product counterfeiting
- 7.2 Introducing a simple method of validation for customs inspection
- 7.3 Developing an inspection tool or security feature that assists in identifying suspected or spurious electronic equipment and components
- 7.4 Providing assurance to end users
 - 7.4.1 Case Study – Retail Packaging with security hologram – D-Link Wireless Router for PC
 - 7.4.2 Case Study – BBC News Story – Warning - Fake ‘Jemella ‘ghd’ Brand Hair Stylers in Britain
 - 7.4.3 Case Study - Schreiner ProSecure have developed a product protection system with Hair Styler Brand Owner Jemella ‘ghd’
- 7.5 Is it possible to develop a single, global anti-counterfeit device that will be recognised and used in all applications?
- 7.6 Applying the right strategy and tactics to anti-counterfeiting and anti-tampering initiatives
- 7.7 Developing a layered approach to product protection
 - 7.7.1 A layered approach to authentication
 - 7.7.2 Case Study – Tamper evident and authentication labels for Intel CPUs
- 7.8 The importance of being able to prove provenance
- 7.9 How install a resilient and adaptable system

- 7.10 How to protect against theft in the supply chain and on the retail shelf
- 7.11 Marking packaging so that products can carry their own self-validating features
- 7.12 Adapting paper labels
- 7.13 Using swing tickets and tags
- 7.14 Adapting primary packaging and adding tear tapes
- 7.15 Forensic (invisible) marking methods and compounds for products and components
- 7.16 Direct Visible Marking methods for Electronics components
- 7.17 Security labelling (base) materials
- 7.18 Security packaging (and cap sealing) materials
- 7.19 Security tags and swing tickets
- 7.20 Adding security laser engraving
- 7.21 Specialist security materials for use in the electronics sector
- 7.22 Brand Protection Features
 - 7.22.1 Special Inks
 - 7.22.2 Embossing, Holograms and foils
 - 7.22.3 Films and overlays (includes polarisers)
 - 7.22.4 'Chipless' tags
 - 7.22.5 Radio frequency (RFID) devices
 - 7.22.6 Digital watermarking (printed encryption) and covert codes carried on-pack
 - 7.22.7 On product marking to aid verification
 - 7.22.8 Ink jet marking
 - 7.22.9 Transfer ribbon marking
 - 7.22.10 Laser encoding – on product and ink activated
 - 7.22.11 Linking serial marking to authentication databases
 - 7.22.12 Using the internet and SMS messaging to provide provenance advice
 - 7.22.13 Product marking with encrypted (2D) bar codes
 - 7.22.14 Surface feature identification
 - 7.22.15 Protecting brands on the world wide web

- 7.23 Cost and relative security performance measurement
- 7.24 Summary - Suitability of security technologies for a variety of packaging components
- 7.25 Opportunities for Manufacturers of Brand Protection Solutions – Electronic Equipment and Components

Appendix I Brand Protection Solutions – A new series of 10 targeted end user sector specific market reports from Vandagraf International

Appendix II Major multi-client report: The International Markets for Brand Protection Solutions – 2nd Edition (Publication date: January 2008) - A techno-economic market review

About Vandagraf International Limited

Author Profiles

Acknowledgements.