

BY DANIEL B. HONIGMAN // STAFF WRITER

# 10

## MINUTES WITH . . . BRAND-DEFENDER AND SCAM-SLAYER **IRFAN SALIM**, PRESIDENT AND CEO OF MARKMONITOR

**POP QUIZ: WHAT** does the term “brandjacking” mean? If you thought of the fake Gucci purses for sale on New York City’s Canal Street, you’re right. According to the Organisation for Economic Co-operation and Development, the total value of counterfeit goods represents about \$650 billion annually.

What you may not know is that 14% of it, or \$84 billion, is being sold via unauthorized online channels, and that’s where Irfan Salim and San Francisco-based MarkMonitor step in. With more than 14 billion Web pages on the Internet and countless e-mails sent each day, it’s safe to say brand marketers have a lot of online on their minds. Brand monitoring programs like MarkMonitor help keep track of not just what’s being said about clients’ brands but their overall brand security, by checking the Web for abuses of a brand and taking steps to end the abuse.

Salim spoke with *Marketing News* about brandjacking and fraud of all kinds—not just fake Gucci purses.

### Q&A

**Q:** Who’s at risk for brandjacking and why?

**A:** In a classical marketing sense, any product that has a high brand equity and has a high cost-of-sale is at risk, and it’s amazing how broad that risk is. You wouldn’t think brandjacking happens with automotive parts, but counterfeit parts get manufactured and sold every day. The automotive parts business loses about a billion dollars because of this each year.

The losses aren’t just in revenue, but in brand equity and, eventually, customer trust. If

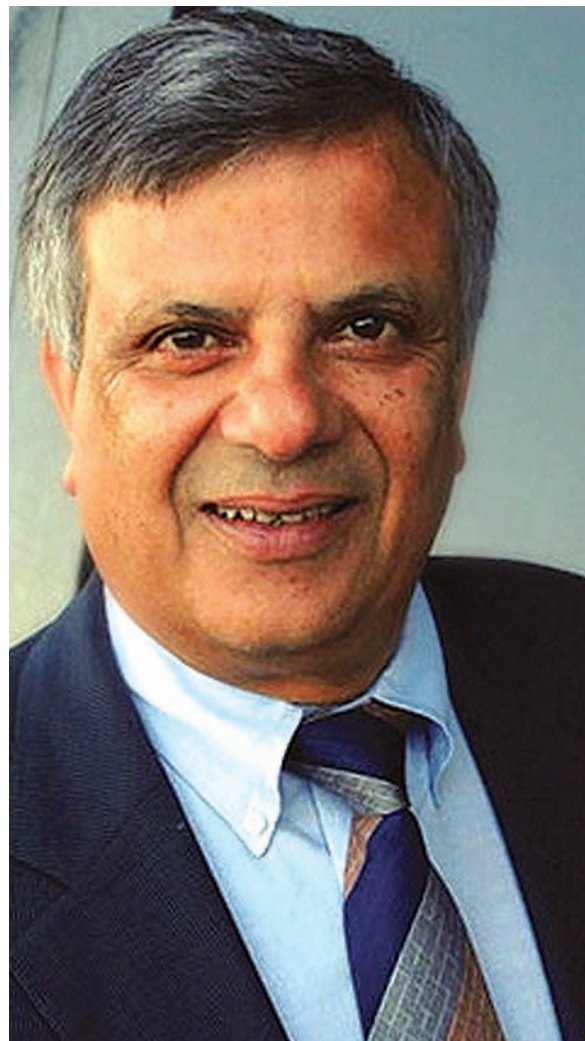
you look at big brands in financial institutions, [identity theft] eventually leads to less trust in a brand. You can take brands that are physical products [or] non-physical products like electronic transaction products and they are all at risk [for] brandjacking.

**Q:** From a marketing standpoint, what can a company, or even an entire industry—like online pharmacy sales—do to pull itself back up if brandjacking occurs? Is there a set course of action?

**A:** The first thing is to be aware that as your business model has moved online, so have the bad guys.

Part of what brand owners do to protect their brand in the physical world is to package with holograms, lasers and radio-frequency identification. They do authorization of distribution channels where they look to train dealers. They also have physical security of premises.

But what are they doing equivalent to those efforts online? Very little. The focus of online security has been more on data and





# A matter of trust

59% of C-level executives trust print media over online news sources, according to a Doremus/*Financial Times* study.

network protection, but there's the massive, but intangible, brand asset [that] comes with managing your image online. Be aware of the risks your brand faces online. Next, be organized when you address it, and that's where brand owners face their biggest challenge.

**Q:** Is there a rule of thumb that outlines the percentage of one's marketing budget that people should spend on brand security?

**A:** What I can articulate is the dimension of the problem in some elements that are highly measurable. [One estimate of the size] of the online market for fake goods is about \$110 billion. There's fraud in pay-per-click that may be as high as 20%.

The biggest challenge is hard to measure, and that's just part of marketing: How do you measure brand awareness and brand asset value? What happens if a customer completely loses trust in your brand?

**Q:** So the metrics involved with brandjacking are metrics that any marketer would use to measure a campaign? What are the metrics for brand security?

**A:** I think in general, campaign management metrics are still just as subjective as the campaign objectives themselves. People have tried to apply science, but many times it comes down to having a warm feeling that your campaign works.

[With brand security], I think there are harder metrics. How much loss prevention can you implement in online channels? Is it shutting down unauthorized sales of your product or identifying fake products and stopping the sale of that? Those are hard metrics that you can drive ROI from. The same is true for your advertising budget ... you may be able to improve the productivity

of the dollars you spend online by 10% if you can reduce your cyber-squatting and traffic diversion by 20%.

**Q:** Marketers aren't necessarily techies, so when it comes to monitoring brand identity use and abuse online how does the technology work?

**A:** It's a software-as-a-service model where information regarding your brand is presented to you in prioritization of actionable items. The fundamentals are what we call the 'four A's' of brand protection platforms:

First, you have to acquire the data about your brand on the Web, which ... may include spam, URLs with mention of your brand and so on. We have technology to search not just your brand name but the context in which it's mentioned. We also have relationships with major ISPs, where we get about 16 million URLs fed through our system.

Then you want to analyze [the data]. If I hit you with 14 billion instances of your brand being mentioned, you won't find it useful. We do correlation engines and risk scoring and we can identify if your brand is being abused in writing, but we also can tell when your logo is being abused on the Web.

The other two layers are simple: We announce brand abuse and broadcast data to major Web browsers like Internet Explorer 7 and Firefox. We call this "fraudcasting"

The last layer is to be able to act, and [herein lies] a lot of different elements. If you identify site 'x' that hasn't been approved to sell your product or is selling fake products, there are legal steps we can automate. There's a whole process ... to shut down a domain. We can automate those steps and then we partner with physical security companies that can do surveillance and shut down fake factories.

**Q:** So what's the next danger brandjack-

ers pose that marketers will have to face? What's the next wave?

**A:** Here's the irony of the whole thing: The criminals are not only clever from a technology point of view, but they're actually architecting better and better marketing campaigns. If you think about it, their focus is to get a user to click on a URL and then to act. In classic marketing, when you have banner ads or sponsored links, you want to know how many people went there. This is exactly what the bad guys are trying to do. Better design of e-mails and Web sites to make it look like it comes from a company—that's social engineering and they're doing that. Then you have people deploying anti-spam technology to block e-mail, but the bad guys are always figuring out clever ways to get through the spam filters.

The most recent tactic is that [criminals] are making it harder to locate them so you can't take action. For instance, in a study we did of the pharmaceutical industry, we saw that many brandjackers appeared to be in Canada but then saw they were actually in Russia. They hijack servers and then hide behind multiple layers [of security].

**Q:** It sounds pretty complicated.

**A:** I'm telling you, the bad guys are just as clever, if not more clever, than the good guys. To put it in perspective, if you talk about IT security, viruses started in the late '80s, early '90s, then hacking [became popular]—all of this stuff happened in the last 10 [or] 15 years. Before that, there were no chief security officers in organizations, and most organizations [still] haven't organized to address the threat to [their] brand online. When you look at protecting your brand, it's a big challenge. **m**

# MarkMonitor®

Reprinted with permission from the American Marketing Association