# **Fake News, Real Problems:** Combating Social Media Disinformation

ALEXANDER BOOTH

**Associate Managing Director**

**Business Intelligence and Investigations**

**London, UK**

abooth@kroll.com

BENEDICT HAMILTON

**Managing Director**

**Business Intelligence and Investigations**

**London, UK**

bhamilton@kroll.com

MARIANNA VINTIADIS

**Managing Director, Southern Europe Head**

**Business Intelligence and Investigations**

**Milan, Italy**

mvintiadis@kroll.com

Social media is a powerful tool for brand building and communication—and a double-edged sword that can cause significant damage in the hands of an adversary.

Brands have been valuable assets since before the first trademark was granted. For much of that time, companies were able to control and shape their brands through their marketing, advertising and other communications strategies. Today, however, social media has transferred much of that control to online communities. Under the right conditions, a small band of loyalists can grow virally into a dedicated following and give a company or a cause a global presence seemingly overnight. But adversaries ranging from competitors to short sellers can harness the same platform to hijack the reputation of a company or one of its employees through fake news stories, malicious posts and other underhanded tactics, as illustrated by these recent Kroll engagements:

After an African bank was purchased by a rival institution, the purchaser was confronted with a negative social media campaign, complete with fabricated news stories and manipulated closed-circuit television footage. The instigators turned out to be a group of shareholders of the acquired bank who had opposed the sale.

An employee of an authorized repair center of a global automobile manufacturer found her social media page filled with photos of herself and her children that had been photoshopped onto pornographic images. The perpetrator was identified as a disgruntled customer, who was subsequently arrested.

A fast-growing U.S. cosmetics company suddenly became the target of a barrage of Twitter attacks falsely claiming that its products were tested on animals, which caused sales to drop by 20 percent. The cascade of negative messaging was traced back to a rival company's head of marketing, who had hoped to depress the competitor's share price.

As with other types of threats, like cyberattacks or physical security breaches, early detection and quick response are essential when a company or brand faces an online disinformation campaign. This is particularly true at the moment, when even countries with well-functioning legal and regulatory systems are grappling with the question of what restrictions on social media are appropriate. Companies thus need to arrange for ongoing monitoring of online sentiment and have predetermined strategies for countering disinformation when it appears. Knowing the source of the story—and thus the underlying motivations of the other side—often provides useful raw material with which to develop effective counter-messaging.

While online disinformation is a global phenomenon, the regions in which an organization does business may increase its vulnerability to such attacks. For example, regions that combine a young, cyber-literate population and a mainstream media with weak editorial standards will find that it is easier for misinformation to migrate though mainstream channels once it has been established online. Absent an effective court system, parties in a dispute may feel they have little to lose by waging an aggressive battle in the court of online public opinion. Alternatively, having a vibrant industry press covering the intersection of the internet with law, business and society helps keep the public informed of online threats and scams.

Social media can be a powerful vector for fraud as well as disinformation. In one recent case, an ultra-high-net-worth individual had one of her social media accounts hacked when her password was guessed based on the hobbies she posted about. In addition to harassing the individual by posting embarrassing material on her page, the intruders were able to access her email account and read exchanges between her and her bank. Based on this information, the intruders sent emails to her bank mimicking her writing style and directing a transfer of funds. Fortunately, the bank became suspicious and did not make the transfer. Nonetheless, this series of events demonstrates how a social media breach can have far-reaching consequences. Indeed, the ubiquity of digital communication, combined with an always-on work culture, means that access to personal accounts can easily expose sensitive business information. Because of this, companies should ensure that employees are taking appropriate social media precautions, including the following:

1. Establish separate business-facing and personal social media accounts—and consider using only a first name in the latter. Don't post anything in one that can be linked to the other.
2. Use randomly generated passwords at least ten characters in length.
3. Disable GPS metadata for social media posts.
4. Educate family members regarding defensive social media behavior.
5. Periodically review social media posts and delete anything that could be used in damaging ways. If the post has not been commented on or saved by others, deletion is likely to keep it from view.

Social media's value as a communications channel will only continue to grow. Both individuals and companies expend considerable effort in leveraging that channel, but they must also take defensive measures to ensure that the channel does not become a weapon turned against them.