

CORPORATE MISINFORMATION AND FINANCIAL HOAXES

Innovative Solutions
to Face Arising Risks

June 2023



Foreword

Many companies and mainstream media outlets face a growing challenge. How to ensure trust in an era of escalating misinformation? Publicly listed companies and financial institutions are the most exposed to these rising threats. It is quite a challenge in the era of chatbots and other AI applications.

Financial fake news directly impacts the value of the companies involved. Fabricated news campaigns create harmful effects not only on a company's reputation but also on its financial stability and on its shareholders interests.

There are numerous ways to manipulate corporate information. In this white paper, we assess their level of sophistication, from a simple forged press release to complex schemes to gain access to well-protected IT systems or to generate "artificial" content thanks to new AI applications. When it comes to finding loopholes for profit, the ingenuity of hackers is limitless. Especially when the objective is to make quick money with limited risks, like manipulating cryptocurrencies' value through fake corporate announcements (see the Walmart case below).

In a recent study entitled *Market manipulation and suspicious stock recommendations*(1) the academic Thomas Renault specifies: "*The channels most used by fraudsters to spread false information are fake press releases (73.3%), followed by fake emails or newsletters (34%) and fake websites (32%)*".

The authors of those attacks not only have numerous techniques, they also follow various motives. Some are novice or seasoned activists trying to raise awareness for their cause. Those hoaxes are some of the most efficient tools in their influence arsenal. The YesMen became famous after their Blackrock hoax. On January 16, 2019, they sent out a fake annual letter to investors and journalists signed by Larry Fink, CEO of BlackRock, hours before the release of the real letter.

The fake letter announced that the world's leading asset manager would sell out its investments in the fossil fuel industry in compliance with the Paris Agreement. An astonishing pledge that managed to fool mainstream media outlets like the Financial Times.

Other fraudsters use fake corporate communication to manipulate the market and engage in insider trading schemes. The gains generated by those sudden variations on the stock market can make them rich in minutes while being difficult to trace.

A factual analysis is essential to understand how to anticipate and better face these rising threats. This white paper includes a selection of recent hoaxes and fraudulent attacks that were covered by the media. Those use cases depict the landscape of "corporate news hacking."

Blockchain technology to combat fake news

Wiztrust's team of experts have gathered numerous factual cases of corporate hacks to design a solution to help corporations protect their communications. Those findings led them to develop Wiztrust Protect®.

Wiztrust Protect®(2) is the European certification and verification platform of corporate information. As such, it partners with Euronext that promotes its usage among European listed companies. Wiztrust harnesses the cryptographic power and inalterability of blockchain technology to allow companies to certify their communications. Journalists and investors can then verify in real time the authenticity of the financial information by a simple drag and drop of the content onto www.Wiztrust.com.

Recent innovations in the digital world disrupt corporate communication for better and for worse. They allow fake content to spread instantly. With AI chatbots, identifying the authentic source of a content becomes impossible.

We also believe that new technologies can be the right solution to fight fake news

(1) <https://www.thomas-renault.com/wp/market-manipulation-suspicious.pdf>

(2) <https://www.wiztrust.com/en>

Summary

Real time information, Real time threats	<i>Page 6</i>
The motives : Activism & Profit	<i>Page 8</i>
A recent hack Case : Adidas	<i>Page 10</i>
Dark PR, troll factories and AI disinformation technologies	<i>Page 12</i>
Corporate fake news publication, who is responsible ?	<i>Page 14</i>
The risks: low costs, large consequences	<i>Page 16</i>
An acceleration of corporate disinformation cases	<i>Page 18</i>
BlackRock & AP7 hack cases	<i>Page 20</i>
Q1 2023 hack cases	<i>Page 24</i>
AI chatbots: Where is the source ?	<i>Page 26</i>
Fake tweets: insuline is now free !	<i>Page 28</i>
Takeaways for PR officers & journalists	<i>Page 29</i>
Blockchain as a solution: Here comes the sources again!	<i>Page 30</i>

Real time information, Real time threats

The speed at which information is circulated constantly accelerates. Business media, especially financial news agencies, have little to no time to check the authenticity of a piece of news or press release. AI amplifies the issue as an increasing volume of content is produced by bots that are publishing articles without any human involvement and no way to check who's the source of a content.

With the rising level of distrust towards the media, journalists are in a critical situation when they face highly sophisticated information hacks. These are difficult to detect, especially when coupled with perfectly mirrored websites, realistically spoofed emails, and fake press releases. Checking an official-looking document becomes a time-consuming task in a world of real time.

Corporate communication is shared through multiple channels, via a press release sent through an official email address, a newswire, a tweet, or in a newsroom on the company's official website. Unfortunately, when official communication responsibilities are scattered throughout several teams such as PR, social media, digital, employee communication... achieving perfect synchronization becomes impossible. Hackers have learned to take advantage of those little delays a journalist might overlook.

Fake CCOs ?

We observed that corporate information hackers have refined their methods since the first major hoaxes, 15 years ago, and now combine most, if not all, those communication channels. A well-prepared attack often involves a fake press release sent through a fake yet similar email address, with a link sending the recipient to a spoofed newsroom on a mirrored website with a typo squatted hijacked URL. For the most elaborate attempts, those documents even include a phone number, leading to a corporate voicemail or answered by a fraudster pretending to be part of the PR team or even the CCO of the company as in the AP7 case(3). Even a trained and meticulous journalist might be fooled by the apparent confirmation of the fabricated news. Not to mention the use of different time zones that makes verification difficult while PR executives and journalists are sleeping...

Verification is even more costly when it comes to critical news. Having the exclusivity on such information, even for a couple of minutes, is both a matter of reputation and revenue for the media company. “Hacktivists” exploit this urgency to deceive journalists into relaying apparently legitimate fake news on social media, and sometimes in reputable media with a wide audience.

Surprising or expected announcements

Our inventory of use cases reveals that impostors bait journalists with carefully crafted content to tease their thirst for a news exclusive. A substantial share of fraudulent communication materials sent out by fraudsters are about extraordinary, unpredictable events that would require immediate coverage and urgent crisis communication.

When they are not betting on surprise, many hackers do exactly the opposite. In several cases, they sent spoofed press releases right before a very anticipated event or deadline, such as the publication of an annual letter to investors or of a company’s financial results. Those attacks take advantage of the expectations of journalists and their finance-savvy audience. A press release covering a planned event or a recurrent communication landing in a journalist’s inbox on the right day has greater chances to escape scrutiny. A journalist rushing for the buzz might overlook those little discrepancies.

This verification work is even more critical since a fake information relayed by one media outlet, especially a reputable one, can be spread by many others. This chain reaction is amplified by social networks, where any news article, video, tweet or post from a journalist can be shared and commented by thousands of people in a matter of minutes. As MIT researchers stated in a study recently published in *Science*⁽⁴⁾, fake news tends to spread even faster and wider than real information.

(3) <https://www.thelocal.se/20200701/extinction-rebellion-claims-responsibility-for-swedish-pension-fund-hoax>

(4) <https://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308>

The motives : Activism & Profit

In most of the cases we listed, cyber-activism and greed are the main motives behind corporate fake news.

Corporate communication hacking is a very efficient scheme for activists to gain media coverage for their cause. The manipulation of official information is also a way to highlight one company's little-known controversial activities, to mock a brand, to damage a business' reputation, to influence its management or to call for a boycott. This is often referred to as simple "PR pranks" or "hoaxes." The recent Adidas case is a good illustration of this kind of hoaxes.

Activism

The YesMen, an activist group expert in spreading fake news, has targeted several multinationals(5). As an example, a fake GE press release or a fake and expected Blackrock's CEO's newsletter were sent to the media. More recently, they manipulated Vanguard's communication to showcase the alleged doubtful environmental behavior of the asset manager.

Extinction Rebellion, the civil disobedience movement fighting against ecological collapse and global warming(6) has targeted the Swedish pension fund, AP7. The activist group sent out a false press release to several international media. Last summer

Galp group in Portugal was subject to information manipulation combining a fake announcement and street activism to denounce its involvement in Mozambique.

Greed

Greed is a powerful driver of corporate communication hacks. Financial misinformation is a lucrative market. When the hoaxes are not promoting some social or political message, fraudsters try to influence and manipulate the market, benefiting from the sudden upward or downward slides produced by a breaking news only they could expect. This form of "induced" insider trading generally targets public companies of various sizes: from traditional "pump and dump" on penny stocks to complex schemes influencing some of the biggest names on the world's leading exchanges.

A "pump and dump" scheme is an attempt to make easy and quick profit in markets with high volatility. A fraudster would first acquire a large quantity of cheap "penny stocks" of a small company before spreading fake or exaggerated positive news on the market to drive the stock price up and sell out those stocks at high price to more gullible investors, driven by the fear of missing out on a potential gold rush.

Hackers may sometimes use this mechanism in the opposite way. A fraudster would first take bearish positions on an asset and spread negative news to artificially drive its value down. The hacker could then buy the stocks back in, share a spoofed denial statement or wait for an official one to be issued in order to profit off the stock's recovery.

In both cases, gains can be quick and massive. The use of derivative products following a whole index or basket of assets can make those fraudulent profits nearly untraceable. Moreover, when the manipulation involves volatile crypto currencies (as in the "Walmart case"), crooks can make money in a few minutes while being impossible to unmask.

Those market manipulation techniques are typically not new and they could also include more basic forms such as financial spamming through emails or fabricated newsletters. Nonetheless, new media habits and technologies as well as high-frequency trading considerably amplified and accelerated their effects.

(5) <https://theyesmen.org>

(6) <https://rebellion.global>



A RECENT HACK CASE

Sportswear giant Adidas was targeted by a fake press release on January 16th, 2023.

The fake release from activist group Yes Men announced the nomination of a Cambodian union worker as co-CEO.

The activists also organized a fake event in Berlin.

"Berlin fashion spoof causes chaos as Adidas denies involvement"

The Guardian

"Adidas says Berlin Fashion Week launch and co-CEO announcements are fake"

CNBC



Certified with
wiztrust 

What happened ?

- A fake press release sent by the Yes Men announced the nomination of Cambodian union worker to the position of Adidas co-CEO on January 16th, 2023.
- A second fake release promoted the fake "Realitywear" line of clothing, made of clothes distressed by working conditions in Adidas factories.
- The fake press releases were available on a domain-squatted website copying the official group website (adidas-group.eu instead of adidas-group.com).
- A Berlin event showcasing the fake new line of clothing took place at the same time.
- A third fake press release denying the first two was also sent, adding to the confusion.

The hoax intended to highlight working conditions in Adidas factories in Cambodia.

Its goal was to put pressure on the company to sign the Pay Your Workers agreement promoted by the Clean Clothes Campaign.

A corporate spokesperson denied the nomination and the company's involvement in the event, stating that « this announcement is not by Adidas and not correct. »

Dark PR, troll factories and AI disinformation technologies

In recent years, many fake news distribution schemes have been attributed to "dark PR" companies. Two-thirds took place since 2020 illustrating an acceleration of the phenomenon. There is now a new industry of more or less official PR firms and marketing agencies ready to deploy fake stories and pseudo news websites. These "communication professionals" organize disinformation operations on behalf of anyone who can afford to buy their services.

Business models built on deception

"The professionalization of deception is a growing threat," said Nathaniel Gleicher, head of cybersecurity at Facebook. We have seen agencies establish themselves and build most of their business model around misinformation." (7)

Some agencies publicly announce on their website that they use all available tools to twist reality as the client wishes. Up to now, Dark PR companies relied on 'troll factories. Battalions of human content producers connected to fake Facebook accounts to comment or guide conversations. Even though Facebook regularly announces the deletion of many accounts run by disinformation agencies, dark PR continues to thrive on social networks.

The distinction is sometimes tenuous between dark PR agencies and troll factories. Some agencies use fake Twitter and Facebook accounts to serve their clients. They use the terms "additional pages" and "digital support workers" to describe what are otherwise known as "fake news sites" or "paid trolls".

AI and the automation of large-scale disinformation

One of the latest shift in the dark PR sector consists is AI powered disparagement or destabilization campaigns. We see the emergence of agencies that leverage new technologies and become specialists in large scale manipulation of information. Kinds of disinformation mercenaries equipped with state-of-the-art AI tools.

The production of disinformation is based on automatic content generation software or robots. The so-called fake content "Farm Automatic Collection Systems" reorganize the words and sentences of certain articles to produce endless new texts and thus (attempt to) manipulate the search engines. Indeed, artificial intelligence does not only allow, like ChatGPT, to create various contents. It also makes it possible to produce large quantities of viral content in seconds, to put articles, posts or tweets online, in the language of your choice, and to distribute them automatically and at high speed via Facebook, Twitter or Instagram. This trend is denounced and described in details by Forbidden Stories, the platform of the association of journalists Freedom Voices Network(8).

Confronting dark PR ?

The global PR industry is combating the rise of dark PR. The industry took a stand against social media manipulation when the PRCA expelled Bell Pottinger, a London-based PR agency, after investigating misinformation campaign it staged in South Africa for one of his clients(9).

Weber Shandwick's CEO told BuzzFeed that her agency needs to *"engage the public with information grounded in truth, even when the agency is competing in markets where dishonest tactics take place."* ICCO, the worldwide organization of public relations consultancies, has established 10 principles known as the Declaration of Helsinki(10). They demand that communication professionals "be aware of the power of social media and use it responsibly" and "never engage in the creation or dissemination of false information".

As major PR agencies strive to differentiate themselves from disinformation practices, platforms find it increasingly difficult to prevent dark PR from invading their ecosystems. *"If an agency works on multiple platforms for many different clients, we may not be able to destroy them completely,"* says Facebook's Gleicher. *We want to make it very clear that this is not a sustainable business model on our platform"*

(7) <https://www.zdnet.com/article/disinformation-for-hire-pr-firms-are-the-new-battleground-for-facebook/>

(8) <https://forbiddenstories.org/story-killers/team-jorge-disinformation/>

(9) <https://www.theguardian.com/business/2017/sep/04/bell-pottinger-expelled-from-pr-trade-body-after-south-africa-racism>
row#:~:text=Bell%20Pottinger%2C%20one%20of%20the,of%20ethics%20in%20its%20history

(10) <https://iccopr.com/helsinki-declaration/>

Corporate fake news publication, Who is responsible ?

Fake financial news proliferate and a question agitates the media landscape: beyond the hackers and the activists of disinformation, who of the “issuing company” or the journalists should be held responsible for it? On the one hand, the media are experiencing an influx of information that needs to be processed and disseminated as quickly as possible. Faced with this mass of press releases, many journalists are struggling to juggle between verifying the authenticity of the information and the need to publish it as soon as possible. This phenomenon is amplified for the financial press agencies whose robots take over the information in real time.

Best practices to prevent liability

Jurisprudence shows the responsibility of the media in these situations. We can cite the conviction of Bloomberg which, after having taken up a false press release, had been ordered to pay a five million euros fine at first instance by the AMF(11). The verdict was confirmed on appeal with a slightly lower fine.

This could be surprising because, on the other hand, the Autorité des Marchés Financiers describes what it expects from companies issuing information in article 221-4 of its General Regulations(12). This states that *“Regulated information is transmitted to the media in its entirety and in a manner that guarantees security of transmission, minimizes the risk of data corruption and unauthorized access and provides certainty as to the source of the information transmitted”*.

From this point of view, the issuing company has obligations in terms of security and traceability of its information, if only to prevent its shareholders from paying the price of manipulation. In fact, it could be held responsible if it does not adopt good practices, especially if activist investors challenge the management for its lack of foresight.

The liability related to the publication of corporate fake news in the economic sector is therefore a growing concern.

All the stakeholders can be implicated, from the issuer of the information to the media. The dissemination of press releases in an archaic way, via unsecured mailboxes, creates an ideal ground for hackers and activists. In these cases, communications teams' thoughtlessness could be interpreted as sheer carelessness. Clearly identifying the source of news is more critical especially since investors monitor social media to follow the "sentiment" of the crowd, a kind of new "social consensus", and adapt to it as quickly as possible.

(11) <https://www.amf-france.org/en/news-publications/news-releases/enforcement-committee-news-releases/amf-enforcement-committee-fines-bloomberg-lp-dissemination-false-information>

(12) <https://www.amf-france.org/en/eli/fr/aai/amf/rg/article/221-4/20191122/notes>

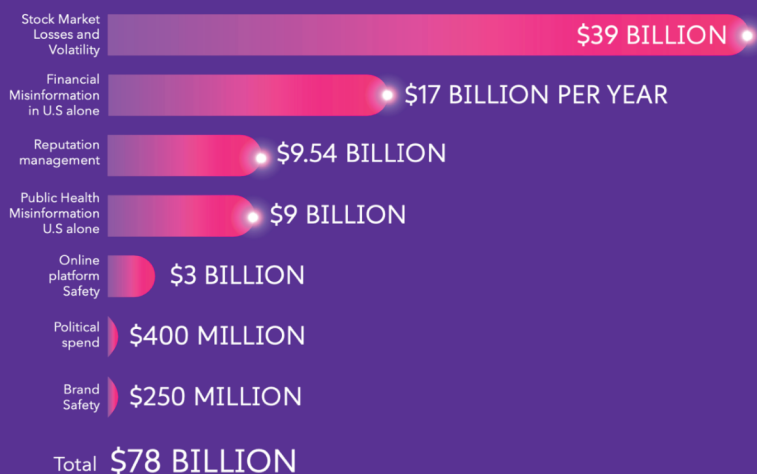
The risks: low costs, large consequences

With limited risks and resources for maximum impact, corporate news hacking is representative of a type of cyberattack on the rise that requires its potential targets to adopt new practices.

The proliferation of corporate communication hacking cases might be partly explained by the asymmetry between the resources needed to undertake such operations on one side and the potential gains of the fraudsters and cost for the targeted company on the other side. Getting a fake press release published requires minimal resources in comparison with the potential backlash that the victim, its brand image and its market valuation might suffer, especially since the authors of corporate communication hacks are rarely identified and arrested.

\$100 versus \$26.5 Billions

Some attacks, with spoofed press releases will “only” damage the brand a company built, making revelations to the public that, real or not, might destroy years of customer relationships, good PR and corporate social responsibility efforts. Others lead to much more quantifiable financial damages. The University of Baltimore evaluated the costs of financial misinformation at \$17 billions and its impact on corporate reputation as \$9.5 Billions(13)



Those losses highly contrast with the estimated costs of the hack. Sending a fake press release is free, making a mirror website of the official one can be learned in a short time, hosting costs the hacker roughly \$20, answering the fake phone number to impersonate a PR officer and confirm the news only requires a \$10 prepaid phone card.

Taking a high estimate, the total cost of the attack probably amounts to less than \$100.

Cryptocurrencies as an accelerator

More recently, false announcements of retailer-cryptocurrency collaborations have gained momentum. Hackers have once again shown the impact of communication and its weakness in the face of cyber threats. Fake press releases claiming that the company would allow cryptocurrencies as a new payment option were distributed last September by “fake” Walmart communication teams. The information provoked a huge increase in the cryptocurrency’ value. The hackers made millions in a few minutes and will probably never be found.

Finally, the judicial remedies are extremely limited. While the SEC and other financial regulators around the world can launch investigations, the odds of finding out the identity of the hackers are low. Instead, they end up issuing new guidelines that can only postpone the next big hack.

Minimal risks, limited resources but maximal impact; corporate communication hacking is characteristic of the most recent cyber-crime techniques. It requires potential victims to preemptively adopt new behaviors and innovative tools in order to prevent risks that will only become greater.

(13) <https://www.ubalt.edu/news/news-releases.cfm?id=3425>

An acceleration of corporate disinformation cases

2022, a peak year for fake news

The 2000 Emulex hoax, when a Californian optic fiber manufacturer lost 62% of its stock value following a fake press release, is one of the first major corporate communication hack that garnered public attention. Information manipulation techniques have rapidly evolved since then. We decided to list here a short selection of some of the most characteristic cases of corporate news hacking of the past decade. Some made it to the front page of the newspapers, especially when they were an activist endeavor to gain coverage. Others remained under most radars, handled as silently as possible to cover a hacker's tracks or to protect the target company from greater undesirable effects. Between 2000 and 2018 we identified "only" a few cases par year. The acceleration started then and never stopped. Today similar cases happen every week.

TESLA

On April 2022, a fake press release was heavily relayed by Tesla fans on social media, mostly Twitter. The car manufacturer was announcing the buy-out of Lithium Corporation, a specialist of the extraction of the metal. The news was made credible by a statement made shortly before that Tesla might be interested in an acquisition in this sector. Lithium Corporation's stock jumped by 250% until the company published a "real" press release denying the previous announcement.

Vanguard®

A first fake press release was sent to Earthier by a hacker. This press release touted a new fossil-fuel-free portfolio it called "Vanguardians of the Galaxy". A few hours later, another press release showed up claiming to be from Marvel saying the Vanguard announcement would "mislead customers into believing they would make their investment products 'real zero' and 'Paris-compliant'". Both fake press releases had contact (phone number and email) and a website created a few days before (investor-vanguard.com and news-marvel.com). The Fixers activist group sent actors disguised as Guardians of the Galaxy to distribute flyers. The dueling press releases were actively shared on Twitter to drive attention of people eager to see Vanguard greenwashing.

Walmart

A fake press release was distributed mentioning that Walmart would now accept Litecoin cryptocurrency as for payment. The fake press release was part of a pump-and-dump scheme intended to hike up the price of Litecoin and sell it off for a profit. News of the purported partnership caused Litecoin to jump by 32% in just 25 minutes. The Security & Exchange Commission opened an investigation.

galp

A fake press release was sent out by Portuguese activists stating that Galp Energia was abandoning its involvement in oil exploitation in northern Mozambique to pursue a "100% renewable future". The communication director's identity was usurped and the fake news was disseminated using a fake but credible email address. The hoax occurred on a 1st of April and was quickly refuted by Galp. In the meantime, major Portuguese media had relayed the false information.

Denbury

Denbury Resources was the victim of a fraudulent news release. An announcement was sent out on behalf of Denbury about a \$1.20 a share buyout offer for the struggling company. The company's shares spiked nearly 47% to 33 cents in premarket trading, before closing at 26 cents a share, up about 12%. The share price had nearly tripled just before the listing was suspended.

SoftBank

Softbank was the victim of a fake press release announcing the launch of a crypto wallet card, a kind of debit card which embedded IoT chips to make it "smart". As the news seemed legitimate, a lot of media outlets picked up the story such as AP news, Block Crypto, Coin Telegraph, Business Telegraph and more. As of today, this mystery remains yet unresolved, and the investigation continues.

HACK CASE

"Hoaxsters sent out a fake annual letter pretending to be from BlackRock's influential CEO Larry Fink"

CNBC

"BlackRock target of hoax claiming big move on Paris climate deal"

Axios

"Someone wrote a fake letter pretending to be BlackRock CEO Larry Fink and some reporters got duped"

Business Insider

"BlackRock falls victim to 'brilliantly executed' hoax over 'sin stock' assets"

The Telegraph

"The fake Larry Fink that duped reporters"

Institutional Investor



What happened ?

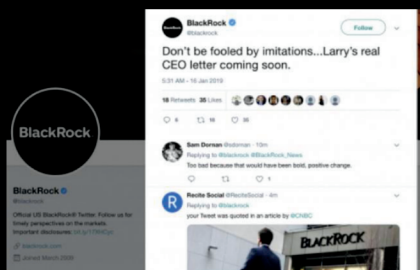
January 16, 2019

- 6:15 AM : The day Larry Fink was expected to publish his annual letter, a fake letter was sent using a fake email address (larry.fink@blackrock-esg.com) to reporters.
- Enclosed the fake letter was titled "Larry Fink's Annual Letter to CEOs : Purpose in action"
- The fake letter linked to a fake website using the company's identical layout with exact logos and colors. (BlackRock-esg.com)
- The activists also paid for Google ad space to have the fake letter appear at the top of related searches. They also generated fake Twitter accounts to confirm the fake news.
- 08:20 AM : The Financial Times, tricked by the fake letter and website, published a headline announcing, "BlackRock to dump companies failing to comply With Paris accord".
- 08:31 AM : Using the same mediums as the Activists, BlackRock confirmed the letter to be a hoax on Twitter and via email, to reporters more than the 2 hours after the attack

Who fell for the fake ?



Denial





HACK CASE

What happened ?

The AP7, Sjunde AP-fonded, a government agency which manages premium pension fund for the Swedish people was hacked by Extinction Rebellion (XR) purporting to be the fund itself and distributing false information to Media outlets.

The activists sent a press release in English and Swedish, presented according to the brand's graphic chart, to several media outlet internationally. The press releases led to a fake website, which was a copy of the real one.

The fake news mentioned that the fund had taken the decision to divest from the fossil fuels industry and would become carbon neutral by 2030.

One of the activists, contacted by AFP for confirmation, even posed as the real spokesperson for the AP7 fund, Johan Florén, giving journalists credible details. The false spokesperson told AFP: *"We believe that the risk of investing in fossil fuels will increase in the future"*.

Who fell for the fake ?

The false information was picked up by several media outlet such as IPE, one Swedish website, the french news agency AFP, and many international news outlets syndicating the AFP story.

What happened next ?

AP7 filed a complaint for the action of "disinformation". The real Johan Florén commented :

"When disinformation becomes on ordinary method, with fakes sites, false reports and even people pretending to be someone else, it's not just journalism that will suffer. People will also suffer. Citizens will give up and stop trying to make informed and democratic decisions, when no one will know what is wrong or not".

The statement made by the hackers

"On Monday the 29th of June we, activists of Extinction Rebellion, sent a press release posing as Swedish state governed pension funds AP7. In the release we claimed that AP7 was to divest ownership in all companies with operations in fossil fuel. Unfortunately, that is not true. We sent the press release that AP7 should have sent".

Headlines

"Sweden's largest pension fund swears off fossil fuels"

Yahoo

"AFP NEWS – Extinction Rebellion claims hoax about Swedish fund"

Barrons

"AP7 to report fossil fuel divestment hoax to police"

IPE

"Extinction Rebellion réussit une action de désinformation contre les médias"

La Tribune

"Comment Extinction Rebellion a fabriqué une fausse information pour servir sa cause"

Les Échos

Q1 2023 hack cases

A brief selection

TESLA

CNEVPOST

Tesla refutes reports of \$25,000 Model 2 as fake news

By Phate Zhang/CnEVPost
February 14, 2021 10:19 GMT+8

Reports that Tesla is developing a \$25,000 vehicle are circulating widely among Chinese Internet users today. In response, Tesla has dismissed them as fake news.

Several Chinese media outlets reported that Tom Zhu, president of Tesla China, confirmed that the company is working on a cheaper Tesla for the mass market, with an estimated retail price of 160,000 yuan (\$25,000).



Post-Courier
The Independent of PNG

TOP STORIES

Fake Media Release Not From BPNG

March 15, 2023

BY MAXINE KAMUS

Bank of Papua New Guinea confirms that the letter released stating that the Bank of PNG will grant a license to Golden Sun PNG Limited is fake.

The Central Bank said as per their protocols, the format for the letterhead is incorrect and the Governor does not sign on press releases or any other information shared with the public.



Dragon Gate Investment Partners Statement L...

Dragon Gate Investment Partners Statement in Response to Fake DataCanvas Press Release


September 07, 2022 21:30 ET | Source: Dragon Gate Investment Partners [Follow](#)

New York, Sept. 07, 2022 (GLOBE NEWSWIRE) -- Dragon Gate Investment Partners was the subject of a fake news release issued on Wednesday, Sept. 7, 2022, that falsely stated Dragon Gate Investment Partners led the new



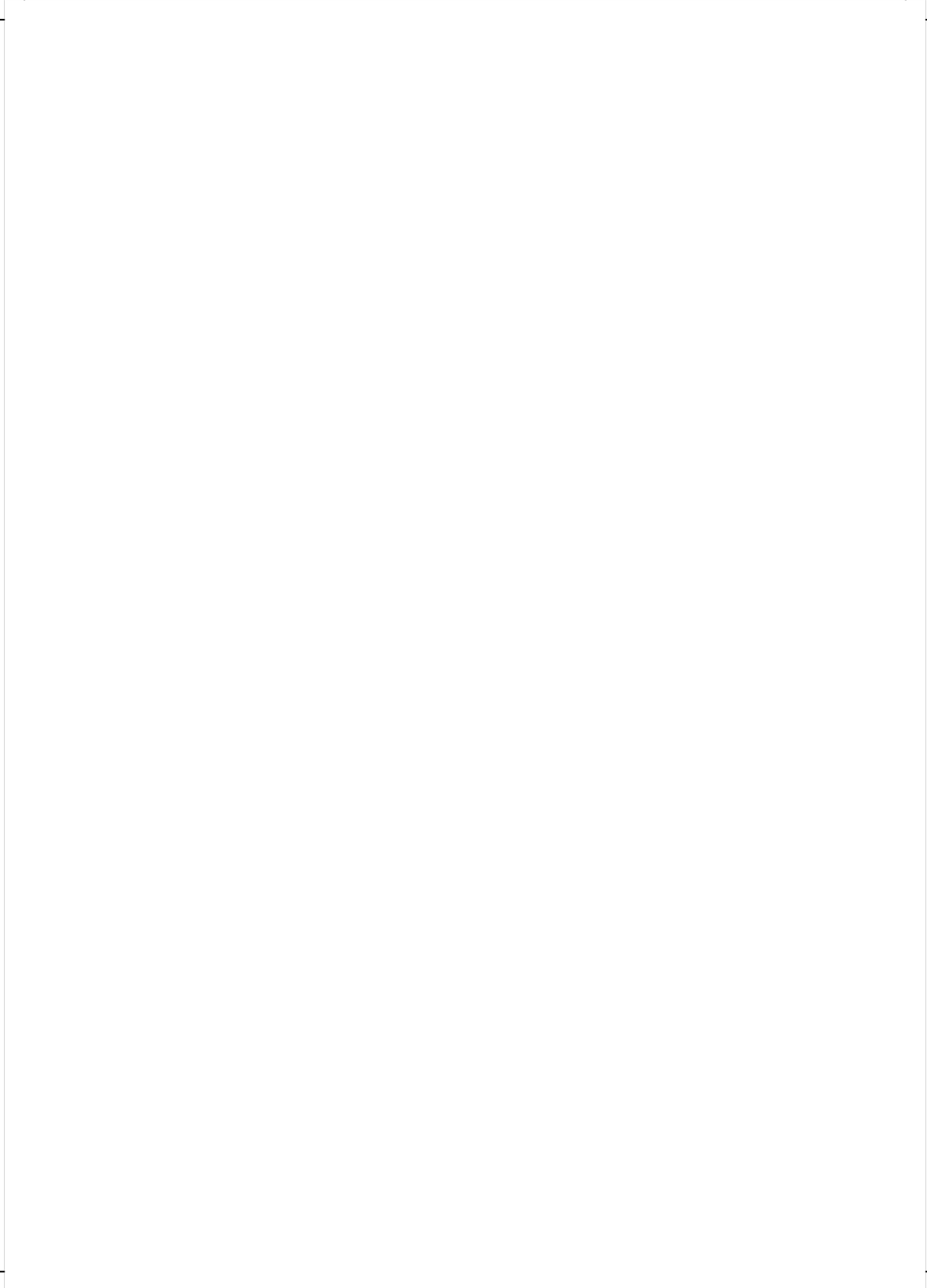
Robert Scammell
PROPTech / THU 20 APR 2023

Revealed: The lies exposing Letting Cloud's fake Airbnb acquisition



Letting Cloud CEO Grant MacCusker

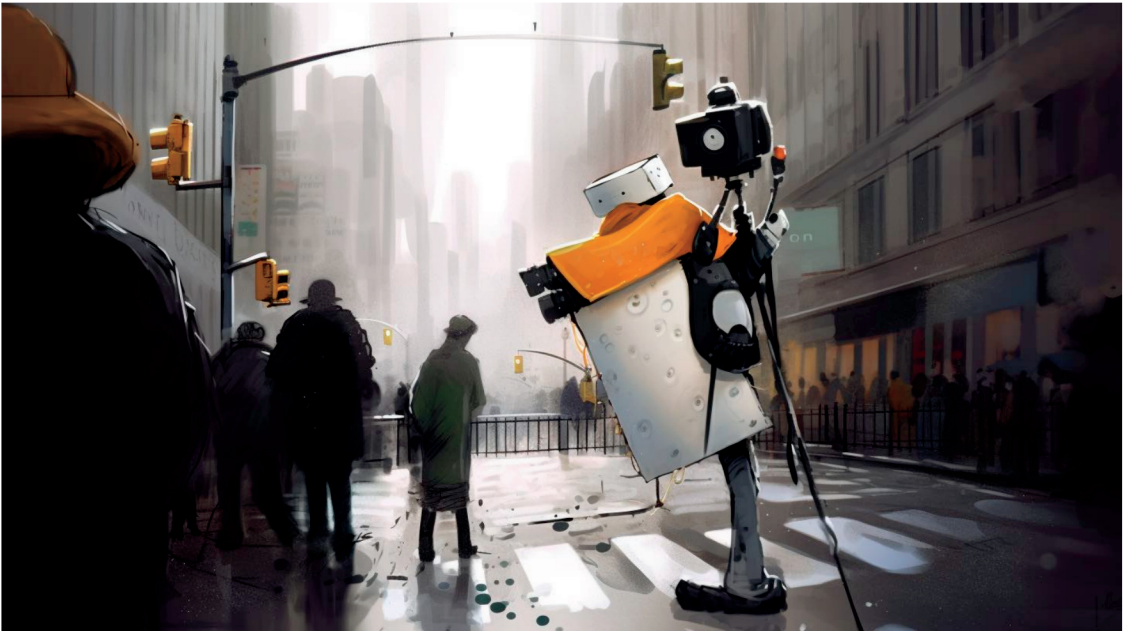
Airbnb's 'acquisition' of Letting Cloud was entirely fabricated by the Scottish proptech company's CEO and founder, a UKTN investigation can reveal,



AI chatbots: Where is the source ?

It was hours after the launch of new generative AI tools like OpenAI's ChatGPT, Microsoft's BingGPT and Google's Bard that it became clear that they would have a huge impact on the spread of misinformation.

Regulators and technologists have been slow to recognize the dangers of fake news on social media and mainstream media. They are still trying to catch up. Now experts are sounding the alarm as more and more examples of inaccurate generative AI robotic content circulates. *"It's getting worse and faster,"* said Gary Marcus, an AI-skeptical professor of psychology and neuroscience at New York University(14).



An image of a robot taking picture generated by AI software Midjourney/ Reuters Institute

In fact, generative AI tools like ChatGPT, Dall-E or Midjourney have no idea of the boundary between fact and fiction. They also tend to make things up when trying to accommodate human users' desires. One of the biggest threats posed by AI-generated misinformation right now is malicious actors exploiting the tools to spread false narratives quickly and widely.

Misinformation can flow both to and from AI models. First, this means that some generative AIs will be subject to "injection attacks," where malicious users teach lies to programs, which they then pass on.

Another challenge is the threat of misinformation from everyday users unintentionally spreading lies. *"The technology is impressive, but not perfect... Anything that comes out of the chatbot should be approached with the same kind of scrutiny that one might get from replying to a random tweet,"* said to Axios Jared Holt, senior research director at the Institute for Strategic Dialog⁽¹⁵⁾.

Tech companies are trying to address potential industry and regulatory concerns about AI-generated misinformation by attempting to detect fake news and using feedback to train algorithms in real time. NewsGuard recently launched a new misinformation prevention tool to enable generative artificial intelligence services to collect data on the web's most trusted news sources and disregard the most prevalent fake news. Generative AI vendors can use the data to better train their algorithms to avoid false narratives. Microsoft already licenses NewsGuard data and uses it for BingGPT. At Microsoft, user feedback is considered a key element in improving how ChatGPT works.

The challenge, however, is that end users lose interest in determining the authenticity of a source...because the source is intangible. They no longer care about the origin of the content and trust the information as soon as it is available. *"Average users also need to be aware of bias, said Chirag Shah, a professor at the University of Washington School of Information, which is especially difficult for users to detect with ChatGPT-generated responses with no link to the source..."*(15)

⁽¹⁴⁾ <https://www.economist.com/by-invitation/2023/04/18/the-world-needs-an-international-agency-for-artificial-intelligence-say-two-ai-experts>

⁽¹⁵⁾ <https://www.axios.com/2023/02/21/chatbots-misinformation-nightmare-chatgpt-ai>

Fake tweets: insulin is now free !

Pranksters taking advantage of Twitter's relaxed rules to get "verified" accounts are flooding the app with fake posts from companies, often hitting their stock prices. Lilly recently fell 4.5% after someone used a "verified" account designed to look like the company's official social media channel to tweet: *"We are pleased to announce that the insulin is now free"*. The release not only affected the pharmaceutical company's share price, but also those of rival insulin makers Novo Nordisk (NVO) and Sanofi (SNY).

Lockheed Martin fell 5.5% due to a fake "verified" account claiming to reveal: *"We will start stopping all arms sales to Saudi Arabia, to Israel and the United States"*. Other fake messages using "verified" accounts designed to appear official included an alleged message from PepsiCo (PEP) that *"Coca-Cola is better."* Poland Spring's parent company, Nestlé, appeared to admit that *"we stole your water and we're giving it back to you"*.

It happened as well to Elon Musk. A fake SpaceX Twitter account has appeared to reveal that *"it is with heavy hearts that we announce that we will be suspending all missions. We plan to funnel \$240 million in government grants to groups dedicated to sustainable agriculture and ending world hunger"*. These issues led Twitter to remove its new option to offer verified accounts and to launch a new certification system. The old blue checkmarks are gone.

The social network has just officially launched its new "Verified Organizations" subscription, which allows companies to request the new golden badge, but also to certify their employees. All from €950 per month! At this price, you benefit from the basic subscription, allowing you to obtain the golden label, as well as the square avatar, specific to companies/organizations. Each Affiliate Certification will be charged an additional \$50 each month. A company wishing to affiliate 10 employees will therefore have to pay the sum of €1,450 to Twitter each month.

The instability of Twitter is causing an exodus of brands that cannot trust the platform to protect their interests. *"A lot of brands have been hijacked,"* Ari Lightman, a professor at Carnegie Mellon University, told Gizmodo⁽¹⁶⁾. Confidence is now replaced by a bit of fear and pessimism about what's next and what these changes could really mean for brands in the long run.

(16) <https://gizmodo.com/twitter-airlines-air-france-klm-air-travel-1850418687>

Takeaways for PR officers & journalists

The analysis of the selected cases, whether they have been orchestrated by fraudsters or activists, reveals a few insightful trends.

- In all cases, journalists published the information with insufficient fact checking, lacking the time or the means to do it properly. When they tried to verify the authenticity of the fake material with a routine check on the linked newsroom or a quick call to the contact number, they were tricked by the fake website or fake press relations services set up by the attacker.
- When a news agency or trustworthy media shares the information, it validates and grants the fake information with new levels of legitimacy. Readers and even other media will be much less likely to check it.
- Content crafted by fraudsters is false yet always plausible, even in the most far-fetched hoaxes.
- Hackers' favorite medium is, by far, the press release, whose traditional format is easy to efficiently spoof at roughly no cost.
- The channels used to spread misinformation are generally multi-tiered: fake emails, fake newsrooms or websites, fake phone numbers... This combination of various levels engineered to give the appearance of truth makes the traditional verification work useless if the person who undertakes it does not personally know the author of the information.

Blockchain as a solution: here comes the source again!

There are several methods to convey fake news, of varying technological complexity, from sending a false statement via an ordinary email to more sophisticated hacking of the information systems of market authorities, through the manipulation of several information channels. The imagination and ingenuity of activists is limitless in drawing attention to the cause they defend. These malicious pranks or hoaxes are among the best tools in their arsenal of influence. This is a phenomenon that we are closely analyzing for Wiztrust Protect© our blockchain based corporate content certification platform(17).

Trusted relationships

The challenge is to ensure that the source of a document is authentic and that the document has not been altered. The "traditional" way to do so is that PR teams build trustworthy relationships with the media. This is a basic in public relations: to call key journalists in advance to inform them of an important announcement and/or be available to answer questions with no delay. This is obviously a good way to prevent disinformation ... if the media knows the PR team, has the personal phone number of the corporate PR people, and if the announcement is in the same time zone. PR pros tend to sleep in London when a critical (fake) announcement is made in Hong Kong.

In fact, journalists must be able to quickly and easily check the source and integrity of any communication material, at any time even if they do not know the corporate communication team personally. The success of the verification process thus depends both on the good practices of media professionals and on the company's ability to properly certify its content, then to make the verification accessible with as little time and effort as possible.

Certification technology

As the preliminary step before verification, the certification process must be permanent, impossible to spoof or falsify while staying easily accessible for the verifying party. Furthermore, to keep control of the time of publication and avoid official information leaks, the certification process must keep the content of document secret and only confirm the integrity and source of a document submitted by the verifier.

Finally, it is essential to clearly separate the verification process from the document itself, since a fake document can link to a fake verification interface the same way it can refer to a fake PR team contact number.

Wiztrust Protect© allows companies to realize such a certification process in a couple seconds, harnessing the blockchain's distributed ledger immutability and cryptographic security features. With just two clicks, any corporate communication team can anchor the "metadata" of a press release, a report or a picture. Journalists can then easily verify on [Wiztrust.com](https://www.wiztrust.com) the certified source of the content. Blockchain is in fact the most reliable way of ensuring trust in corporate information and protecting stakeholders, in particular shareholders, from fake financial news.

Multi-channel simultaneous news distribution

Multi-channel communication is also a great complement to certification for a company willing to mitigate the risks. It is far more difficult for a hacker to spoof convincingly or to gain access to 5 or more communication streams (email, newsroom, website, newswire, social media...), rather than just a couple of them. A company that uses a communication platform such as Wiztrust PR to distribute simultaneously its official information through many different channels is making potential fraudsters' lives much more difficult.

As communication evolves with emerging technologies, trust in corporate and financial information is becoming the number one priority for journalists, analysts and investors. Financial institutions and public companies, especially their communication and PR leaders, must innovate to match these new expectations, secure their reputation and protect their shareholders.

If new technologies boost the spreading of fake news, it is also through them that one can find the solution.

(17) <https://www.wiztrust.com/en>



Wiztrust is the publisher of Wiztrust PR and Wiztrust Protect®, the first fully secured and compliant software suite to help financial institutions and publicly traded companies manage their communication. Wiztrust users can easily manage and certify their content, publish them across all their communication channels and track their performance, in a simple and secure interface.

Jérôme Lascombes

Co-Founder and President

jerome@wiztopic.com

Raphaël Labbé

Co-Founder and CEO

raphael@wiztopic.com



PARTNER OF

