COMPREHENSIVE RESPONSE TO RECENT SHARE PRICE VOLATILITY

London, England and San Francisco, CA – 31 March 2014 – blinkx plc ("blinkx" or the "Company") provides a detailed response and its perspective on a blog published about blinkx on 28 January 2014, ("the blog"), which contributed to the recent volatility in the Company's share price.

blinkx strongly refuted the assertions made in the blog at the time it was published. Since then, the Company has completed a thorough investigation of these assertions, including:

- A comprehensive internal review of current procedures and processes across blinkx;
- An audit of the Company's technology and processes by Kroll, the Global Leader in Risk Management; This audit was led by the Head of the Cyber Investigations and a former FBI Special Agent with extensive industry experience in online investigations, brand protection and internet traffic forensics;
- A legal review of the Company's practices and commercial obligations by the law firm DLA Piper, LLP, as related to the FTC's (Federal Trade Commission) enforcement actions. This review was performed by a Partner and former FTC investigator and included a proactive outreach to the FTC's Division of Advertising Practices and Division of Enforcement, within the Bureau of Consumer Protection;
- An outreach to Harvard University to understand the University's policies governing the non-academic research activities of faculty and potential conflicts of interest relating to the paid for publication and marketing of such financial research to institutional and retail investors; and,
- Engagement with relevant financial regulatory authorities to investigate the recent trading activity and volatility in the Company's shares.

Through this publication, the Company expands upon the numerous factual errors in the blog, which follows the four primary sections contained in the blog. The Company has been able to confirm and verify that the blog contains materially misleading information, uses selective data, makes erroneous assumptions about current and past practices, and reflects either a fundamental misunderstanding of the online advertising ecosystem and economics or is a deliberate attempt to use partial, incorrect and misleading information to arrive at subjective and malformed conclusions.

As a publicly traded company in a rapidly changing industry, blinkx management and Board are acutely aware of their fiduciary duty to investors. To that end, blinkx has always welcomed an informed debate about the Company in which ideas are shared openly to help form investment decisions, and the Company would never seek to curtail such an important function played by commentators.

However, given the apparent errors and bias within the blog, the subsequent disclosures that still remain opaque particularly around potential sponsorship and the short position in blinkx stock built prior to the blog, the Company questions the motivations and transparency of both the blogger and the sponsors of his research, who may have made significant financial gains as a result of the adverse impact on blinkx's share price. Included below is an unedited version of the blog alongside blinkx's detailed response to each assertion advanced by the blogger.

Blog Assertion:
Video and advertising conglomerate Blinkx tells investors its "strong performance" results from "strategic initiatives" and "expanding demand, content, and audiences." Indeed, Blinkx recently climbed past a $1.2 billion valuation. At first glance, it sounds like a great business. But looking more carefully, I see reason for grave doubts.

My concerns result in large part from the longstanding practices of two of Blinkx's key acquisitions, Zango and AdOn. But concerns extend even to Blinkx's namesake video site. In the following sections, I address each in turn. Specifically, I show ex-Zango adware still sneaking onto users' computers and still defrauding advertisers. I show the ex-AdOn traffic broker still sending invisible, popup, and other tainted traffic. I show Blinkx' namesake site, Blinkx.com, leading users through a maze of low-content pages, while charging advertisers for video ads systematically not visible to users.

blinkx Response:
blinkx has consistently represented that it is a B2B Tech-Media company with unique strengths in video, but that video is not the only thing blinkx does. Rather, the Company has a diversified set of digital advertising capabilities and integrates multiple online ad formats to move from selling ad units to ad campaigns. While video is the past, present and future of the Company, sufficient scale, scope and reach to compete effectively is a fundamental requirement to succeed in the online advertising industry. Virtually every step the Company has taken since its inception in 2004, when online video was still "buffering" has been to further this agenda, whereas the video and video advertising market did not go mainstream until years later. This has included significant investments in technology, products, people, processes and acquisitions. While aspects of the product lines the blogger highlights are integrated into our operations, the blogger combines unrelated past practices, such as those relating to Zango prior to acquisition of specified assets by blinkx, with erroneous inferences about our current practices in order to draw our business model into question and paint an unflattering picture of the Company. Each of the blogger's assertions is discussed in detail below.

1. The Legacy Zango Business

Blog Assertion:
In April 2009, Blinkx acquired a portion of Zango, a notorious adware vendor known for products that at various times included 180 Search Assistant, ePipo, Hotbar, Media Gateway, MossySky, n-Case, Pinball, Seekmo, SpamBlockerUtility, and more. Zango was best known for its deceptive and even nonconsensual installations -- in write-ups from 2004 to 2008, I showed Zango installing through security exploits (even after design updates purportedly preventing such installations by supposed rogue partners), targeting kids and using misleading statements, euphemisms, and material omissions, installing via deceptive ActiveX popups. These and other practices attracted FTC attention, and in a November 2006 settlement, Zango promised to cease deceptive installations as well as provide corrective disclosures and pay a $3 million penalty.

blinkx Response:
It is important to understand that a) blinkx did not acquire Zango and b) the period referenced above not only pre-dates blinkx, but also refers to an era in the industry that underwent significant change after 2008. blinkx acquired specific assets of Zango out of a foreclosure sale from a consortium of banks on April 16, 2009. Concurrent with the asset acquisition, blinkx also hired a number of ex-Zango staff into the blinkx organization. Zango, like many other companies of its kind ran an innovative and highly successful online advertising business that used an ad-supported software distribution model, until lax oversight of rogue partners and related activities destroyed its business model. While some of the ad units may be seen as intrusive (as are TV ads, which interrupt the viewing experience), they do not violate any laws when presented appropriately with requisite disclosures. The entire content economy (TV, magazines, web sites, mobile apps, etc) is rooted in this fundamental principle, whereby the user watches ads in exchange for access to quality content. The ad-supported software business that blinkx runs today complies fully with industry standards and requirements for the distribution and monetization of desktop and mobile ad supported software and applications. The business further provides blinkx with an important test bed for new technology, distribution and ad units. Since the acquisition and integration of the ex-Zango assets, specific processes and procedures, particularly around consent, choice and uninstallation, have been significantly revamped in order to meet or exceed current industry standards. Current practices bear no relation to the ex-Zango practices that led to FTC action in 2006 that, incidentally, Zango largely remediated in the three years prior to blinkx's acquisition of assets in 2009.

To address the most egregious assertions in this section of the blog, blinkx engaged outside Counsel represented by DLA Piper to proactively contact the FTC on behalf of the Company regarding blinkx's ad-supported software business. We contacted both the Assistant Director of the Division of Advertising Practices in the Bureau of Consumer Protection and the Assistant Director of the Division of Enforcement in the Bureau of Consumer Protection, to determine whether any aspect of the former FTC Consent Order would carry over to blinkx.

The Division of Advertising Practices is charged with enforcing rules and regulations that relate to unfair or deceptive advertising and marketing practices. As a matter of policy, the FTC does not and will not, publicly or in writing, confirm or deny any ongoing or planned investigations. However, the Assistant Director of this Division communicated to our outside counsel that she was not aware of any application of the Zango Consent Order to blinkx and she indicated that blinkx was not the subject of any current investigation by her Division. In a subsequent

conversation, she further indicated that none of blinkx or its subsidiaries was the subject of any current investigation by her Division.

The Division of Enforcement is responsible for enforcing all consent orders implemented by the Bureau of Consumer Protection, including the 2006 Consent Order with Zango. The Assistant Director of this Division communicated to our outside counsel that he was not aware of any enforcement actions regarding the Zango Consent Order, which means that the Division of Enforcement is not currently alleging that anyone is in violation of the Consent Order. He further stated that he believed the Zango consent order might not be "active" (or still valid) in light of Zango's bankruptcy. Based on his understanding of blinkx's purchase of select ex-Zango assets, he explained that he did not believe the Zango Consent Order would be applicable to blinkx, since blinkx would not be considered a legal successor to Zango.

The above establishes that blinkx rests assured that is not bound by the extraordinary measures leveled upon Zango by the FTC for past practices – validated by outside Counsel, rendering virtually the entire blog section pertaining to this entity null and void.

Blog Assertion:
Few users would affirmatively request adware that shows extra pop-ups, so Blinkx and its distributors use deceptive tactics to sneak adware onto users' computers. In a representative example, I ran a Google search for "Chrome" (Google's well-known web browser), clicked an ad, and ended up at Youdownloaders.com -- a site that bundles Chrome with third-party advertising software. (The Youdownloaders footer states "The installers are compliant with the original software manufacturer's policies and terms & conditions" though it seems this claim is untrue: Chrome Terms of Service section 5.3 disallows copying and redistributing Chrome; 8.6 disallows use of Google's trademarks in a way that is likely to cause confusion; 9.3 disallows transfer of rights in Chrome.) In my testing, the Youdownloaders installer presented offers for five different adware programs and other third-party applications, among them Weather Alerts from desktopweatheralerts.com. Installation video.

blinkx Response:
Ad supported and "freemium" options are valid, recognized and accepted alternatives for packaging and distributing premium content, including desktop and mobile applications, as is the development, use, packaging and distribution of freely distributed and open source software. A majority of the freely available online tools are ad-supported, including toolbars and browser plug-ins, for example. Youdownloaders is a third party distributor and is neither blinkx nor a blinkx affiliate. Rather, the Company appears to be distributing the Weather application (further referenced below), among others noted in the blog via a separate agreement with an approved distributor. Distributors of the Weather application are bound by specific Terms & Conditions of multiple parties, including blinkx, its distributor and publishers of the applications being distributed. blinkx internally monitors distribution partners to ensure Terms and Conditions are being met and if noncompliance is reported or discovered, any such violation of the distribution relationship is reviewed, cured or terminated.

Blog Assertion:
I consider the Youdownloaders installation deceptive for at least four reasons: 1) A user's request for free Chrome software is not a proper circumstance to tout adware. The user gets absolutely nothing in exchange for supposed "agreement" to receive the adware; Chrome is easily and widely available for free, without adware. It is particularly one-sided to install five separate adware apps -- taking advantage of users who do not understand what they are asked to accept (including kids, non-native speakers, and those in a hurry). 2) On the Weather Alerts page of the installation, on-screen statements mention nothing of pop-up ads or, indeed, any advertising at all. In contrast, the FTC's settlement with Zango requires that disclosure of advertising practices be "clear and prominent," "unavoidable," and separate from any license agreement -- requirements not satisfied here. 3) The Youdownloaders user interface leads users to think that the bundled installations are compulsory. For example, the "decline" button (which lets a user reject each adware app) appears without the distinctive shape, outline, color, or font of an ordinary Windows button. 4) Users are asked to accept an objectively unreasonable volume of agreements and contracts, which in my testing include at least 14 different documents totaling 37,564 words (8.5 times the length of the US Constitution).

blinkx Response:

As already established, Youdownloaders in not blinkx or any blinkx affiliate. Therefore, the blogger's assertions regarding this distributor have no bearing on blinkx. However, we can offer objective feedback to specific points made in the blog.

The above appears to be either an intentional or naive attempt to establish a perception of impropriety and discredit not only blinkx, but also the entire ad-supported industry. Perhaps most tellingly, the blogger neglects to point out that Chrome is itself ad-supported software distributed by Google. Like others using the ad-supported software distribution channel, blinkx through its partner bids on an (ad) slot for one of its products, just as it does many times daily on a host of search engines, display ad networks, exchanges, etc. blinkx neither dictates what (other) products Youdownloaders distributes nor controls how the distributor licenses or packages these products before presenting them to consumers, so long as blinkx terms and conditions are not violated.

Specifically, blinkx is not privy to any relationship between Youdownloaders and Google for distributing Chrome, which it would appear Google permits, just as it allows handset manufacturers to customize and distribute copies of its ad-supported Android software. It is true that Chrome is easily and widely available for free, without "adware" but, as mentioned above, the blogger fails to note that Chrome is itself an ad-supported product distributed to increase use of the Google's search engine to display ads. It is quite likely that Youdownloaders may have a commercial relationship with Google and has spent significant time and resources to market its product set to drive users to install its package of software applications, using both SEO and SEM techniques, among others. This is neither misleading, nor illegal, it represents one of many competitive avenues that an end user chooses to find and install software applications of their choice. This is simply how marketing and advertising campaigns are executed in the real world.

It is also interesting to note that Google allows the purchase of the Ad word "chrome download" on google.com. Moreover, Google has among the industry's most stringent relevancy guidelines for downloadable software, which it enforces with distributors like Youdownloaders. Details of advertising support for free software downloads are clearly listed in the terms and conditions, in line with industry standards, and the installation video within the blog clearly shows the link to these terms and conditions in the consent screen.

The blogger cites that there were 14 different documents, but does not provide any details either in his blog or his installation video that all such documents were for Weather Alerts. It is more than likely that since there are multiple applications being offered in the package, each individual software application has its own EULA (End User License Agreement), as mandated by the publisher of the software. Ultimately, the scope of user documentation presented is a matter for the owners of the applications being distributed, and the distributor – something outside of blinkx's control in this example. In actuality, the terms and conditions of Weather Alerts are only 6,143 words in length (as measured using Microsoft Word). By comparison, the iTunes Terms and Conditions, which many users agree to, are 14,803 words in length (as measured using Microsoft Word). The entire construct presented in this section of the blog demonstrates a fundamental misunderstanding of the relationship between Youdownloaders, Google and blinkx, and indeed of the entire ad-supported software model in general.

Blog Assertion:
Tellingly, Blinkx takes considerable steps to distance itself from these deceptive practices. For example, nothing on Blinkx's site indicates that Weather Alerts is a Blinkx app or shows Blinkx ads. The Desktopweatheralerts.com site offers no name or address, even on its Contact Us form. Weather Alerts comes from a company called Local Weather LLC, an alter ego of Weather Notifications LLC, both of Minneapolis MN, with no stated affiliation with Blinkx. Weather Notifications' listed address is a one-bedroom one-bathroom apartment -- hardly a standard corporate office. Nonetheless, multiple factors indicate to me that Desktop Weather Alerts ~~is~~ delivers a version of Zango adware. For one, Desktop Weather Alerts popups use the distinctive format long associated with Zango, including the distinctive browser buttons at top-left, as well as distinctive format of the advertisement label at bottom-left. Similarly, many sections of the license agreement and privacy policy are copied verbatim from longstanding Zango terms. Within the Weather Alerts EXE, strings reference 180search Assistant (a prior Zango product name) as well as 180client and various control systems long associated with Zango's ad-targeting system. Similarly, when Weather Alerts delivers ads, its ad-delivery communications use a distinctive proprietary HTTP syntax both for request (to showme.aspx, with a HTTP POST parameter of epostdata= providing encoded ad context) and response (a series of HTML FORM elements, most importantly an INPUT NAME=ad_url to indicate the popup to open). I have seen this syntax (and its predecessors) in Zango apps for roughly a decade, but I have

*never seen this syntax used by any advertising delivered by other adware vendors or other companies. Moreover, when a Blinkx contractor previously contacted a security vendor to request whitelist treatment of its adware, the Blinkx representative said "The client is Blinkx ... Your engine ... was flagging **their** installer package SWA as SevereWeatherAlerts..." (emphasis added). Notice the Blinkx representative indicating that SWA (another Local Weather program, virtually identical save for domain name and product name) is "their" app, necessarily referring to Blinkx. Finally, in a February 2014 presentation, Blinkx CEO Brian Mukherjee included the distinctive Local Weather icon (present throughout the LW app and in LW's installation solicitations) as part of the "Blinkx Ecosystem" -- further confirming the link between LW and Blinkx. Taken together, these factors give good reason to conclude that Local Weather ~~is~~ applications are powered by Blinkx and part of the Blinkx network. Furthermore, in my testing Blinkx is the sole source of advertising for Weather Alerts -- meaning that Blinkx's payments are Weather Alerts' primary source of revenue and primary reason for existence. (Additions made February 13, 2014, shown in grey highlighting.)*

blinkx Response:
This section contains a series of factual errors that either deliberately mislead or exemplify superficial, uncorroborated research that any trained and accredited financial researcher or organization could have crosschecked using publicly available sources. blinkx does not own Weather Notifications LLC, a fact that could have been established by contacting the Office of the Secretary of the State of Minnesota. Ironically, the blogger was forced to redact portions of the blog to correct this factual error that the app "shows Blinkx [sic] ads," following independent verification by media. blinkx does maintain a commercial relationship with Weather Notifications, where the Company provides the monetization engine for this application and others like it. blinkx puts all such software and applications through a series of proprietary and third party tests before approving them for distribution and monitors them on an ongoing basis.

References to the legacy Zango code snippets, processes, terms, methodology and license agreements are immaterial, since blinkx runs its ad-supported software products in a manner fully in line with all applicable industry standards. The entire legacy Zango code base was refactored, along with the evaluation methodology and distribution process for the monetization engine. The references to 180search Assistant in the code base, in non-utility functions, are immaterial but have been removed. blinkx has instituted an industry leading and proprietary methodology to approve, verify and certify apps that meet or exceed existing industry standards. Contrary to the way it was portrayed in the blog, the reference to the interaction with the security vendor (one of many that blinkx routinely and successfully works with) is in fact an example of one of many changes that blinkx has adopted to improve former Zango and industry practices. In this particular case, it appears that the security vendor referenced had a previous relationship with the blogger and may have worked with him in reference to Zango's practices and the FTC. The vendor therefore may have been predisposed to rejecting any outreach by blinkx. Finally, since blinkx does not own Weather Notification LLC, it is free to partner with any organization, and price and distribute its products as it deems fit. The statement about blinkx providing the primary source of revenue and reason for Weather Alerts to exist is disingenuous and wrong.

Blog Assertion:
Meanwhile, Zango-delivered advertising remains a major cause of concern. Zango's core advertising product remains the browser popup -- a disruptive form of advertising unpopular with most users and also unpopular with most mainstream advertisers. Notably, Zango's popups perpetrate various advertising fraud, most notably 'lead stealing" affiliate windows that cover merchant sites with their own affiliate links. If the user purchases through either window, the Zango advertiser gets paid a commission -- despite doing nothing to genuinely cause or encourage the user's purchase. (Indeed, the popup interrupts the user and thereby somewhat discourages a purchase.) At right, I show a current example: In testing of January 19, 2014, Blinkx/Zango sees a user browsing Walmart, then opens a popup to Blinkx/LeadImpact (server lipixeltrack) which redirects to LinkShare affiliate ORsWWZomRM8 and on to Walmart. Packet log proof. Thus, Walmart ends up having to pay an affiliate commission on traffic it already had -- a breach of Walmart's affiliate rules and broadly the same as the practice for which two eBay affiliates last year pled guilty. I've reported Zango software used for this same scheme since June 2004. As shown at right and in other recent examples, Zango remains distinctively useful to rogue affiliates perpetrating these schemes. These rogue affiliates pay Blinkx to show the popups that set the scheme in motion -- and I see no sign that Blinkx has done anything to block this practice.

blinkx Response:

It is important to note that mainstream publishers, such as MSNBC.com and People.com, routinely use the ad formats referred to by the blogger, regardless of his moral disposition toward this advertising format. In fact, TV ads are arguably the most intrusive of all ad formats, yet they work exceptionally well, as evidenced by the $70 billion spent annually on TV advertising. This section of the blog continues to assert that Zango's core advertising product remains the browser popup and that Zango's popups perpetrate various advertising fraud, most notably "lead stealing," as referenced through the Walmart example, insinuating that blinkx enables and fosters such activity. First, the type of ad product referenced by the blogger in this section is one of several that blinkx uses to provide a comprehensive suite of solutions for advertisers. Second, note that the commission paid by the merchant (Walmart) is to one of its affiliates, who is a blinkx advertiser, and not to blinkx directly. As stated in its Advertiser Terms and Conditions, blinkx specifically prohibits the kind of activity referenced above. Moreover, lead stealing is doubly prohibited through the advertiser's own terms and conditions with its affiliates – providing a redundancy and failsafe against such activity. In fact, blinkx does not allow shopping cart or basket targeting, which is the key moment for lead stealing during the online purchasing process. The reference in the blog to the activities of two eBay affiliates last year actually pertains to "cookie stuffing," and not lead stealing as in the assertion regarding blinkx, and any reference to practices dating back to 2004 is meaningless. Finally, given the sheer volume and real time nature of the transactions involved, there is always the possibility of circumventing any technical measures that may be put in place, which is why blinkx has instituted compliance procedures to routinely spot check its systems and processes manually.

Blog Assertion:
Rather than put a stop to these practices, Blinkx largely attempts to distance itself from Zango's legacy business. For one, Blinkx is less than forthright as to what exactly it purchased. In Blinkx's 2010 financial report, the first formal investor statement to discuss the acquisition, Blinkx never uses the word "Zango" or otherwise indicates the specific company or assets that Blinkx acquired. Rather, Blinkx describes the purchase as "certain net assets from a consortium of financial institutions to facilitate the growth of the video search and advertising businesses." If a reader didn't already know what Blinkx had bought, this vague statement would do nothing to assist.

Even when Blinkx discusses the Zango acquisition, it is less than forthcoming. UK news publication The Register quotes an unnamed Blinkx spokeswoman saying that Blinkx "purchased some technical assets from the bank [that foreclosed on Zango] including some IP and hardware, which constituted about 10 per cent of Zango's total assets." Here too, readers are left to wonder what assets are actually at issue. A natural interpretation of the quote is that Blinkx purchased trademarks, domain names, or patents plus general-purpose servers -- all consistent with shutting the controversial Zango business. But in fact my testing reveals the opposite: Blinkx continues to run key aspects of Zango's business: legacy Zango installations continue to function as usual and continue to show ads, and Blinkx continues to solicit new installations via the same methods, programs, and partners that Zango previously used. Furthermore, key Zango staff joined Blinkx, facilitating the continuation of the Zango business. Consider Val Sanford, previously a Vice President at Zango; her LinkedIn profile confirms that she stayed with Blinkx for three years after the acquisition. I struggle to reconcile these observations with the claim that Blinkx only purchased 10% of Zango or that the purchase was limited to "IP and hardware." Furthermore, ex-Zango CTO Ken Smith contemporaneously disputed the 10% claim, insisting that "Blinkx acquired fully 100% of Zango's assets."

blinkx Response:
blinkx on occasion will enter into commercial transactions to further its business needs and is under no obligation to discuss the purpose or plans of such transactions above and beyond its reporting obligations, or react to the unsubstantiated and unqualified comments of parties who were likely not privy to confidential information. As stated earlier, blinkx did not purchase Zango and has never operated any business under the Zango name. blinkx did acquire specified assets relating to Zango out of a foreclosure sale from a consortium of banks on April 16, 2009, approximately three years after FTC action and subsequent remediation by Zango of its business practices. Concurrent with the asset acquisition, blinkx also hired select ex-Zango staff into the blinkx organization. The ad-supported software business that blinkx runs today complies fully with industry standards and requirements for the distribution and monetization of desktop and mobile ad supported software and applications – in particular, regarding procedures around consent, choice and uninstallation. Current practices bear no relation to the ex-Zango practices that led to FTC action in 2006.

Blog Assertion:
Blinkx has been equally circumspect as to the size of the ex-Zango business. In Blinkx' 2010 financial report, Blinkx nowhere tells investors the revenue or profit resulting from Zango's business. Rather, Blinkx insists "It is not practical to determine the financial effect of the purchased net assets…. The Group's core products and those purchased have been integrated and the operations merged such that it is not practical to determine the portion of the result that specifically relates to these assets." I find this statement puzzling. The ex-Zango business is logically freestanding -- for example, separate relationships with the partners who install the adware on users' computers. I see no proper reason why the results of the ex-Zango business could not be reported separately. Investors might reasonably want to know how much of Blinkx's business comes from the controversial ex-Zango activities.

blinkx Response:
As for revenue attribution to specific products, blinkx places equal importance on all of its product lines and acquisitions and seeks to integrate people, processes and technologies into the greater business to derive the benefits from enterprise synergy. Otherwise, Investors would and should question the logic of such acquisitions. Zango assets were acquired in foreclosure, and it is impractical to isolate their impact to the Company. Carry-over technology and staff have been integrated within the broader blinkx ecosystem, which we reference as part of our business and growth strategy. blinkx is under no obligation to expend resources and energy to detail information beyond its regulatory requirements. For philosophical, commercial and competitive reasons, the Company does not feel it is useful or advantageous to share information that it considers sensitive, and chooses not to do so. This position is fully compliant with all applicable standards and regulations and is consistent with and, in certain cases, exceeds the reporting practices of the giants in the industry. Other than to satisfy academic curiosity, blinkx sees no reason to change its reporting strategy or expend resources to research, measure and audit this information.

Blog Assertion:
Indeed, Blinkx's investor statements make no mention whatsoever of Zango, adware, pop-ups, or browser plug-ins of any kind in any annual reports, presentations, or other public disclosures. (I downloaded all such documents from Blinkx' Financial Results page and ran full-text search, finding no matches.) As best I can tell, Blinkx also failed to mention these endeavors in conference calls or other official public communications. In a December 2013 conference call, Jefferies analyst David Reynolds asked Blinkx about its top sources of traffic/supply, and management refused to answer -- in sharp contrast to other firms that disclose their largest and most significant relationships.

blinkx Response:
As an LSE AIM listed company, blinkx is in full compliance with all applicable financial rules, regulations and reporting requirements as described in the latest IFRS Guidelines, and has been audited by Deloitte since the Company's IPO in 2007. We believe that we meet and exceed the standards set by industry giants, and are fully reporting the level of detail required of us. As far as we are aware, no publicly traded industry leader provides the level of disclosure advanced in the blog. More importantly, such separation would artificially segment the business in a manner not reflective of how we view, operate or aspire to grow the business. We have integrated the business and report at the level of conventional and premium revenues. In addition, blinkx's competitive advantage stems from differentiated technology, surrounded by a commercial ecosystem of supply, content and demand partners. The Company views its list of top clients and partners as commercially sensitive information, and does not generally disclose such information for competitive reasons – another practice consistent with that of publicly-traded industry leaders. However, the Company has provided a representative set of key partners in publicly available presentations and materials. In our view, any further disclosure will only satisfy the curiosity of our competitors and cannot, therefore, serve shareholders' interests.

Blog Assertion:
In March-April 2012, many ex-Zango staff left Blinkx en masse. Many ended up at Verti Technology Group, a company specializing in adware distribution. Myriad factors indicate that Blinkx controls Verti: 1) According to LinkedIn, Verti has eight current employees of which five are former employees of Zango, Pinball, and/or Blinkx. Other recent Verti employees include Val Sanford, who moved from Zango to Blinkx to Verti. 2) Blinkx's Twitter account: Blinkx follows just nineteen users including Blinkx's founder, various of its acquisitions (including Prime

Visibility / AdOn and Rhythm New Media), and several of their staff. Blinkx follows Verti's primary account as well as the personal account of a Verti manager. 3) Washington Secretaty of State filings indicate that Verti's president is Colm Doyle (then Directory of Technology at Blinkx, though he subsequently returned to HP Autonomy) and secretary, treasurer, and chairman is Erin Laye (Director of Project Management at Blinkx). Doyle and Laye's links to Blinkx were suppressed somewhat in that both, at formation, specified their home addresses instead of their Blinkx office. 4) Whois links several Verti domains to Blinkx nameservers. (Details on file.) Taken together, these facts suggest that Blinkx attempted to move a controversial business line to a subsidiary which the public is less likely to recognize as part of Blinkx.

blinkx Response:
This is another example of the blogger's attempt to use pseudo investigative and convoluted arguments to foster the perception of impropriety. Through its acquisitions and for commercial purposes, blinkx inherited and maintains a portfolio of legal subsidiaries. Verti Technology Group, a "company" that the blogger calls into question, is indeed a blinkx subsidiary, but is far from the "company specializing in adware distribution" that the blog claims – something that could have been confirmed by a phone call to the Company. Verti Technology Group represents blinkx's consumer application download business, and blinkx operates these products in a manner compliant with all legal requirements, as well as industry standards and practices, particularly around consent, choice and uninstallation.

2. The Legacy AdOn Business

Blog Assertion:
In November 2011, Blinkx acquired Prime Visibility Media Group, best known for the business previously known as AdOn Network and MyGeek. I have critiqued AdOn's traffic repeatedly: AdOn first caught my eye when it boasted of relationships with 180solutions/Zango and Direct Revenue. New York Attorney General litigation documents later revealed that AdOn distributed more than 130,000 copies of notorious Direct Revenue spyware. I later repeatedly reported AdOn facilitating affiliate fraud, inflating sites' traffic stats, showing unrequested sexually-explicit images, and intermediating traffic that led to Google click fraud.

blinkx Response:
As detailed in publicly available documents, blinkx acquired Prime Visibility Media Group, including its subsidiary AdOn Network, in November 2011. This section begins with dated information, including examples and write-ups relating to the 2005 to 2010 calendar timeframe, and bears no relation to current practices. The time period to which the blogger refers was an era in the Industry that is significantly different from the one in which blinkx operates today. Some of the practices and partnerships the blogger references were standard practice at that point in time, and have significantly evolved in the interim. The blogger again appears to mix subjective opinion with dated, irrelevant information and inflammatory references to create the impression of impropriety.

AdOn is a performance advertising network owned by blinkx that serves an intermediary function between audience supply sources and entities looking to procure Internet traffic for a wide range of conversion metrics – from website visits to purchases of a product or service. Like many in the Internet, AdOn traffic is sourced from thousands of partners, including Publishers, App Developers, Content Creators, Intermediaries, Aggregators, Exchanges, etc. blinkx takes a neutral position on the originating source of traffic, which is almost impossible to determine, and instead has built a technological competence in the continuous and real time screening and optimization of all traffic sources to meet advertiser needs and metrics. We believe that AdOn deploys some of the most sophisticated real time filters in the industry to identify and filter adult, invisible and off-screen traffic. It does so by deploying 48 different, proprietary filters across five stages that range from automated checks at search time to statistical analysis and pattern recognition post campaign. Unlike others in the industry, blinkx mandates several of these filters to ensure traffic quality and performance. For Advertisers, AdOn operates a self-service platform with an explicit Disclose, Mandate, Consent protocol and policy. blinkx fully discloses that it draws no judgment regarding traffic origination – traffic from multiple sources can enter the system and "apply" through the series of filters. The Company mandates that certain traffic be universally eliminated (e.g. Adult, Botlists, Blacklists) and requires that partners consent to any combination of voluntary screens and filters, based on their objectives – which range from brand awareness to purchase. blinkx has further partnered with best in breed third parties and services, including Adometry, Fraudlogix, URL Blacklists, Alexa, and MESD Blacklists to refine and bolster AdOn's proprietary high speed trading algorithms. AdOn neither dictates the price nor the quality or volume of traffic that the advertiser

seeks, since the process is completely automated via a two-stage free market auction, which inherently assures pricing efficiency in real time.

Blog Assertion:
Similar problems continue. For example, in a February 2013 report for a client, I found a botnet sending click fraud traffic through AdOn's ad-feeds.com server en route to advertisers.

blinkx Response:
In this instance, the blogger uses selective or incomplete data to arrive at a malformed conclusion regarding the traffic in question. With respect to the February 2013 report referencing a botnet associated with AdOn's ad-feeds.com server, blinkx confirms that the traffic reached its servers based on the posted log, but not what happened subsequently. Once AdOn receives traffic from its multiple sources, all traffic leaves its fingerprint based on log data. However, AdOn keeps this traffic in a "holding pen" while it runs its battery of tests and applies no fewer than 48 filters, during five stages, to assess traffic quality. The log data in the blog omits this key information, making it impossible to assert that the traffic in question was ultimately delivered to the advertiser. AdOn uses its highly sophisticated, real time filters to specifically block large swaths of traffic that do not meet our criteria for quality. Stakeholders in the on-line advertising ecosystem recognize that traffic quality is an industry wide issue and even the most sophisticated technology or processes cannot filter out 100% of bad traffic. To provide a sense of scale, note that AdOn processes well over 1 billion ad requests a day.

Blog Assertion:
In an August 2013 report for a different client, I found invisible IFRAMEs sending traffic to AdOn's bing-usa.com and xmladfeed.com servers, again en route to advertisers. Note also the deceptive use of Microsoft's Bing trademark -- falsely suggesting that this tainted traffic is in some way authorized by or affiliated with Bing, when in fact the traffic comes from AdOn's partners. Moreover, the traffic was entirely random and untargeted -- keywords suggested literally at random, entirely unrelated to any aspect of user interests. In other instances, I found AdOn receiving traffic directly from Zango adware. All told, I reported 20+ distinct sequences of tainted AdOn traffic to clients during 2013. AdOn's low-quality traffic is ongoing: Advertisers buying from AdOn receive invisible traffic, adware/malware-originating traffic, and other tainted traffic that sophisticated advertisers do not want.

blinkx Response:
The blogger's assertion that he found "invisible iFrames" sending traffic to AdOn is misleading. From the blogger's own packet data, we see a reference that the ad in question was in position at 4x117 while the viewable area was 936x593, and furthermore that it was not in an iFrame. Earlier in the packet there is a reference that suggests an "invisible" iFrame, simply because our general practice concerning traffic acquisition is to assume that the audience is invalid until proven compliant. In some cases, Advertisers may willingly or inadvertently suppress iFrame blocks, which we try to correct when brought to our attention. We employ a double walled mechanism to confirm traffic quality, in the event that the real time systems are inoperable due to an unscheduled downtime. Such traffic is temporarily placed in our holding pen and then is rejected. We would consider this a false negative. As for the bing-usa.com domain that the blogger cites in this example, the assertion that AdOn owns this domain is patently false, a fact that could easily have been verified. His mention of "deceptive use of Microsoft's Bing trademark" has no connection with any blinkx subsidiary, and would be between the owner of the bing-usa.com domain and Microsoft. In certain, rare cases, AdOn does allow colocation and redirection of partner sites directly from AdOn servers to help with optimization and speed, as one would expect in any high speed trading environment.

Blog Assertion:
Industry sources confirm my concern. For example, a June 2013 Ad Week article quotes one publisher calling AdOn "just about the worst" at providing low-quality traffic, while another flags "crazy traffic patterns." In subsequent finger-pointing as to tainted traffic to OneScreen sites, OneScreen blamed a partner, Touchstorm, for working with AdOn -- wasting no words to explain why buying from AdOn is undesirable. Even intentional AdOn customers report disappointing quality: In comments on a posting by Gauher Chaudhry, AdOn advertisers call AdOn "the reason I stopped doing any PPV [pay-per-view] ... this is bot traffic", "junk", and "really smell[s] like fake traffic." Of 31 comments in this thread, not one praised AdOn traffic quality.

blinkx Response:

The above statement reflects a fundamental misunderstanding or limited understanding of the online advertising ecosystem and economics. Typically, an inverse relationship exists between price, volume and traffic quality that matches marketing objectives. Traffic that drives awareness or visits to a site is usually traded for say $0.01 per visit, whereas conversion traffic that requires a user to purchase a product or service may cost $1 per visit. Clearly, awareness traffic will not satisfy direct response objectives.

As stated above, like others in the Internet, traffic is sourced from thousands of partners, including Publishers, App Developers, Content Creators, Intermediaries, Aggregators, Exchanges, etc. We take a neutral position on the nature or source of traffic, focusing instead on the continuous and real time screening and optimization of all traffic sources to meet advertiser needs. AdOn is a self-service system, with an explicit Disclose, Mandate, Consent protocol. blinkx fully discloses that it draws no judgment regarding traffic origination – traffic from multiple sources can enter the system and "apply" through the series of filters. We mandate that certain traffic be universally eliminated (e.g. Adult) and require that advertisers consent to any combination of voluntary screens and filters, based on their objectives. blinkx even eliminates a portion of traffic after paying for it, in order to preserve traffic integrity. Quotes attributed to third parties designed to lend credibility to the blogger's arguments in fact show a fundamental lack of understanding of how the industry actually operates.

Blog Assertion:
Recent statements from AdOn employees confirm undesirable characteristics of AdOn traffic. Matthew Papke's LinkedIn page lists him as Director of Contextual Ads at AdOn. But his page previously described AdOn's offering as "pop traffic" -- admitting undesirable non-user-requested pop-up inventory. His page called the traffic "install based" -- indicating that the traffic comes not from genuine web pages, but from adware installed on users' computers. See screenshot at right. All of these statements have been removed from the current version of Matthew's page.

blinkx Response:
Mr. Papke, a former United States Marine, is a tenured, well respected and successful employee of AdOn. blinkx is in no position to control the contents of his social media profile. The offerings of "pop traffic" and "install based" are legitimate products, but the descriptions and conclusions drawn by the blogger of "adware", "undesirable", and "not from genuine web pages" demonstrate a subjectively negative spin and are reflective of neither Mr. Papke's sentiments, nor the appropriate usage of the traffic. In fact, this traffic is of such high quality, demonstrating a user's self declared interest or purchase intent, that it is usually cost prohibitive and infeasible to deploy it for awareness (brand) campaigns, such as video advertising.

3. Problems at Blinkx.com: Low-Quality Traffic, Low-Quality Content, and Invisible Ads

Blog Assertion:
Blinkx's namesake service is the video site Blinkx.com. Historically, this site has been a bit of an also-ran -- it's certainly no YouTube! But Alexa reports a striking jump in Blinkx popularity as of late 2013: Blinkx's traffic jumped from rank of roughly 15,000 worldwide to, at peak, rank of approximately 3,000. What could explain such a sudden jump?

blinkx Response:
The blogger references a report from Alexa in an attempt to suggest a sudden jump in blinkx.com traffic in late 2013. While blinkx does occasionally test traffic and ad formats with Alexa, the company's method of measurement, through a small sample of installed toolbars, may result in sampling bias. In contrast, blinkx traffic reported by comScore, which uses beacons, a more reliable and broad sample base to track websites, shows no major swings for this timeframe. The Company's internal traffic numbers also indicate no unnatural spikes during this period.

Blog Assertion:
In my automated and manual testing of Zango adware, I've recently begun to see Zango forcing users to visit the Blinkx site. The screenshot at right gives an example. My test computer displayed Blinkx full-screen, without title bar, address bar, or standard window buttons to close or minimize. See also a partial packet log, wherein the Blinkx site attributes this traffic to Mossysky ("domain=mossysky"), one of the Zango brand names. It's a strikingly intrusive display -- no wonder users are complaining, about their computers being unusable due to Blinkx's unwanted intrusion. See e.g. a December 2013 Mozilla forum post reporting "my computer has been taken over by

malware, half the links are inaccessible because of hovering links to Blinkx," and a critique and screenshot showing an example of these hovering links. On a Microsoft support forum, one user reports Internet Explorer automatically "opening ... numerous BLINKX websites" -- as many as "20 websites open at one time, all Blinkx related."

blinkx Response:
The blog's assertion of "Zango forcing users to visit the blinkx site" is inaccurate and wildly misleading, since the associated screenshot in the blog is that of blinkx Beat, a desktop video viewing application that runs a curated list of funny, short-form videos, and not of blinkx.com. blinkx Beat also has a screensaver mode in which advertising is shown for a limited period of time around the entry and exit into this mode. Screensaver mode is initiated once the application detects no activity by the user, as tracked by mouse movement or keystrokes. The blinkx Beat screenshot does not represent the "blinkx site." It's a desktop application and users are not shuttled between the two delivery methods and despite high viewability and verification scores that are gaining traction, blinkx has sunset this product line due to lack of advertiser demand. The reference to "mossysky" is the result of a download of blinkx beat through a "Mossysky" software application bundle. As for the unwanted intrusion cited, the examples and critique highlighted actually concern low quality, "content farm" sites that troll support sites and create long tail SEO/SEM terms to trick unsuspecting users into installing perceived malware fixes. These are machine generated templated pages and in this particular case, blinkx is actually a victim, not a perpetrator, of the consumer scam. The owners of these pages/sites churn out high volume posts scamming users into downloading "software" that in many cases is malware itself, thereby compelling users to repeat the behavior that placed unwanted code on their machines in the first place. blinkx receives a very small number of consumer complaints, on average 1 or 2 per month – and promptly walks the consumer through a range of options to help rid their computer of any potential malware.

Blog Assertion:
Moreover, Alexa's analysis of Blinkx visitor origins confirms the anomalies in this traffic. Of the top ten sites sending traffic to Blinkx, according to Alexa, six are Blinkx servers, largely used to forward and redirect traffic (networksad.com, advertisermarkets.com, networksads.com, advertiserdigital.com, blinkxcore.com, and networksmarkets.com). See Alexa's Site Info for Blinkx.com at heading "Where do Blinkx.com's visitors come from?"

Strikingly, Zango began sending traffic to Blinkx during the winter 2013 holiday season -- a time of year when ad prices are unusually high. Zango's popups of Blinkx seem to have ended as suddenly as they began -- consistent with Blinkx wanting extra traffic and ad revenue when ad prices are high, but concluding that continuing this practice at length risks excessive scrutiny from both consumers and advertisers.

blinkx Response:
As indicated earlier, given the unique nature of the Alexa sample base, the traffic patterns may not necessarily be reflective of broader online behavior. blinkx uses a host of sources and techniques, including SEO and SEM to drive traffic to its stable of owned and operated sites, in addition to syndicating its players to thousands of partners. Consequently, the backlinks referenced above are reflective of the operating processes blinkx uses to promote and market its site to consumers, which in turn reflects where blinkx.com visitors originate. blinkx vigilantly monitors these sources to ensure the highest traffic quality possible. As for the use of popups to drive traffic. blinkx continuously tests different ad formats for brand and direct response advertising. The period referenced in the blog appears to coincide with a short test blinkx ran in the UK to repurpose contextual traffic for brand campaigns due to an industry-wide supply shortage. Unfortunately, the test was not successful and abandoned, as the economics of direct response traffic are prohibitively expensive for brand advertisers.

Blog Assertion:
Meanwhile, examining Blinkx.com, I'm struck by the lack of useful content. I used the Google search site:blinkx.com to find the parts of the Blinkx site that, according to Google, are most popular. I was directed to tv.blinkx.com, where the page title says users can "Watch full episodes of TV shows online." I clicked "60 Minutes" and received a page correctly profiling the excellence of that show ("the granddaddy of news magazines"). But when I clicked to watch one of the listed episodes, I found nothing of the kind: Requesting "The Death and Life of Asheboro, Stealing History, The Face of the Franchise," I was told to "click here to watch on cbs.com" -- but the link actually took me to a 1:33 minute home video of a dog lying on the floor, "Husky Says No to Kennel", syndicated from YouTube, entirely unrelated to the top-quality 60 Minutes content I had requested. (Screen-capture video.) It was a poor experience -- not the kind of content likely to cause users to favor Blinkx's service. I tried several other shows

supposedly available -- The Colbert Report, The Daily Show with Jon Stewart, Family Guy, and more -- and never received any of the listed content.

blinkx Response:
This section reflects the blogger's attempt to use an esoteric (site: blinkx.com) and obsolete (tv.blinkx.com) navigation pathway to judge user experience on the blinkx site. blinkx has partnered with over 1,100 professional content providers, from mainstream, global providers to producers of niche content for users seeking videos on a specific long-tail topic. Generally, blinkx does not host the content on its servers, and points rather to the location of the content. The pages cited by the blogger on tv.blinkx.com are form a legacy sub-section of the site devoted to searching for full-length TV shows and movies, either for free on the original publisher site or via a paid service such as Amazon Prime, and are not reflective of the overall experience or content on blinkx.com. The examples of missing content, namely "60 Minutes" and "Colbert Report", concern third party websites out of our control. The "60 Minutes" episode is no longer at its original location – but rather than serving a 404, or "Not Found" error message, which is a HTTP standard response code indicating that the client was able to communicate with the server, but the server could not find what was requested, blinkx redirected users back to a blinkx video results page to optimize the user experience. This example, along with the Colbert example, represent the same navigation path – showing our intent to allow users access to blinkx content or return to a page where video search is fully current. We have since modified the behavior to return a 404 Error and inform the user that the video is no longer available. "The Colbert Report" and other examples linked to Amazon Prime, delivering users to a site where they could purchase the TV show. Affiliate marketing with Amazon, iTunes and Hulu+ was chosen to prevent presentation of "pirated" content while still maintaining our reputation as a source of such individual program information. Additionally, the claim that video advertising begins playing when a user exits a tv.blinkx.com page is completely unfounded, as this described behavior does not match with the tv.blinkx.com user interface.

Blog Assertion:
In parallel, the Blinkx site simultaneously perpetrated a remarkable scheme against advertisers: On the video index page for each TV show, video advertising was triggered to play as I exited each page by clicking to view the supposed video content. Because the supposed content opened in a new tab, the prior tab remained active and could still host a video player with advertising. Of course the prior tab was necessarily out of visibility: Blinkx's code had just commanded the opening of a new tab showing the new destination. But the video still played, and video advertisers were still billed. Screen-capture video.

blinkx Response:
The video link posted is identical to the one associated with the "lack of useful content" allegation above, and the claim that it opens video advertising when closed is completely unfounded. We do not see the described behavior and it does not match with the tv.blinkx.com UX. The use of new tabs instead of re-painting content in the current or active tab is an accepted and recognized option practiced by many, including the giants of the industry.

Blog Assertion:
Industry sources confirm concerns about Blinkx ad visibility. For example, a December 15, 2013 Ad Week piece reported Vindico analysis finding just 23% of Blinkx videos viewable (defined as just 50% of pixels visible for just one second). By Vindico's analysis, an advertiser buying video ads from Blinkx suffers three ads entirely invisible for every ad visible even by that low standard -- a remarkably poor rate of visibility. In contrast, mainstream video sites like CBS and MSN enjoyed viewability rates two to four times higher.

blinkx Response:
It is important to note that common Viewability and Verification standards are still emerging in the industry, regardless of what many vendors may claim. The blog calls into question the legitimacy of blinkx.com, suggesting that the site overcounts traffic and engages in ad fraud, as it does not meet Viewability and Verification standards. As previously stated, only originators of traffic can perpetrate ad fraud. blinkx only originates a portion of its traffic, and is hyper-vigilant regarding the quality and pricing of this traffic source – the majority of which is generated from our ad-supported software and application distribution business. Moreover, the traffic blinkx originates is used primarily for direct response (CPC, CPL, CPA or CPI buys), and is cost prohibitive for brand advertising (e.g. Video Prerolls).

Many vendors provide viewability ratings, each with its own methodology and rating criteria. Based on our analysis of the Vindico product, it appears that AdTricity may have challenges related to player and browser configurations in providing a comprehensive and reliable measure of a publisher's viewability – in particular with respect to iFrame delivery. Because much of our business is built on syndication, the blinkx universal player is delivered in an iFrame – a standard, industry wide syndication format for quick load times. The Company re-launched blinkx.com in January 2013 with iFrame delivery as the sole method, letting us normalize the user experience across our owned and operated properties and broader, distributed publisher base on multiple screens. In contrast to Vindico, many reputable third parties rate blinkx as a quality environment and publisher. The blogger also fails to state that the average industry wide Viewability score for high volume, programmatic video ads is 23% (source: TubeMogul). We consistently rank among the upper quartile for Viewability according to Integral Ad Sciences and Nielsen consistently recognizes over 94% of blinkx audience when validated against Facebook and Experian data. We are contributing to help shape these standards through our work with OpenVV.org as well as our membership in IAB, and work with several leading third party experts to continuously test our audience quality, including Nielsen, comScore, Integral Ad Sciences, Moat, Adometry, Fraudlogix, and Double Verify, among others.

4. Putting the Pieces Together

Blog Assertion:
Comparing Blinkx's revenues to competitors, I am struck by Blinkx's apparent outsized success. See the table at right, finding Blinkx producing roughly twice as much revenue per employee as online video/display ad networks and advertising technology companies which have recently made public offerings. Looking at Blinkx's sites and services, one doesn't get the sense that Blinkx's service is twice as good, or its employees twice as productive, as the other companies listed. So why does Blinkx earn twice as much revenue per employee? One natural hypothesis is that Blinkx is in a significantly different business. While other services make significant payments to publishers for use of their video content, my browsing of Blinkx.com revealed no distinctive content obviously licensed from high-quality high-cost publishers. I would not be surprised to see outsized short-term profits in adware, forced-visit traffic, and other black-hat practices of the sort used by some of the companies Blinkx has acquired. But neither are these practices likely to be sustainable in the long run.

blinkx Response:
Regarding the primary thesis in the blog – that our Revenue/Employee numbers are almost double those of comparable companies – this analysis is based upon inaccurate and selective data. Our Revenue/Employee/Year is approximately 25% better than that of the competition, as defined by the blogger. In FY2013, we ended the year with 255 staff, and generated $198m in revenue. However, we began the year with over 325 staff, for an average of $683K/Employee. Importantly, the analysis contained in the blog failed to take into account staff augmentation due the Rhythm NewMedia acquisition that we completed in December 2013, though such information was disclosed and is publicly available. In FY2014, on a consensus basis of $240m (Source: Reuters), and 350 employees (not including approximately 20 outsourced offshore resources), the number tallies closer to $685K/Employee. The Company is proud of this metric and the performance it connotes, and aspires to do better. It is also important to recall that (a) blinkx was a spin-out, not a start-up, and got a head start in product and technology, for which the Company avoided significant upfront capital and staff expenditure; (b) blinkx is primarily a supply-side, high-tech entity and benefits from scale efficiency difficult to achieve by companies operating on the higher-touch ends of the value chain; and (c) blinkx has worked hard to integrate the acquisitions it made over time in order to benefit from enterprise synergy and has been aggressive about integrating teams and cutting costs. Ultimately, blinkx focuses on quality revenue growth that converts to cash and management has worked hard to optimize the entire business around this principle. We feel the other allegations around lack of distinctive content, adware, forced-visit traffic, and other black-hat practices have been sufficiently disproven in previous sections.

Blog Assertion:
Reviewing Blinkx's statements to investors, I was struck by the opacity. How exactly does Blinkx make money? How much comes from the legacy Zango and AdOn businesses that consumers and advertisers pointedly disfavor? Why are so many of Blinkx's metrics out of line with competitors? The investor statements raise many questions but offer few answers. I submit that Blinkx is carefully withholding this information because the Company has much to hide. If I traded in the companies I write about (I don't!), I'd be short Blinkx.

blinkx Response:
The blogger suggests that blinkx may not be in compliance with regulatory standards for disclosing revenue at a business line level. As stated previously, as far as we are aware, no publicly traded industry leader provides this level of disclosure. More importantly, such separation would artificially segment the business in a manner not reflective of how we view or operate the business. For philosophical, commercial, and operational reasons, we have integrated the business and report at the segment level, namely online advertising, yet we provide additional detail at the level of conventional and premium revenues. Furthermore, as an LSE AIM listed company, blinkx is in full compliance with all applicable financial rules, regulations and reporting requirements as described in the latest IFRS Guidelines, and has been audited by Deloitte since the Company's IPO in 2007. We believe that we meet and exceed the standards set by industry leaders, and are fully reporting the level of detail required of us.

Blog Assertion:
This article draws in part on research I prepared for a client that sought to know more about Blinkx's historic and current practices. At my request, the client agreed to let me include portions of that research in this publicly available posting. My work for that client yielded a portion of the research presented in this article, though I also conducted significant additional research and drew on prior work dating back to 2004. My agreement with the client did not oblige me to circulate my findings as an article or in any other way; to my knowledge, the client's primary interest was in learning more about Blinkx 's business, not in assuring that I tell others. By agreement with the client, I am not permitted to reveal its name, but I can indicate that the client is two US investment firms and that I performed the research during December 2013 to January 2014. The client tells me that it did not change its position on Blinkx after reading my article. (Disclosure updated and expanded on February 4-5, 2014.)

I thank Eric Howes, Principal Lab Researcher at ThreatTrack Security, and Matthew Mesa, Threat Researcher at ThreatTrack Security, for insight on current Blinkx installations.

blinkx Response:
The blog is rife with numerous factual errors and materially misleading information. Since its original publication, the blogger was forced to correct and update the blog and make further disclosures around conflicts of interest that still remain vague and opaque. In addition, we know that the blog was aggressively marketed to the institutional investor and analyst community, and that following its publication, the blogger continued to promulgate his opinions with retail investors. This leads us to question the motivations of both the blogger and the sponsors of his research, and in our opinion may indicate the use of expert network techniques to influence shareholder sentiment and share price. Ultimately, the misapprehensions in the blog could easily have been corrected through publicly available diligence or by asking blinkx for comment.