

**Statement**

**of**

**K. LEE BLALACK, II**  
**Chief Counsel and Staff Director**  
**Permanent Subcommittee on Investigations**

**Hearing On**

***PHONY IDs AND CREDENTIALS VIA THE  
INTERNET - AN EMERGING PROBLEM***

**May 19, 2000**

Thank you Chairman Collins, Senator Levin, and Members of the Subcommittee. Last November, Chairman Collins instructed the Subcommittee staff to examine the availability of counterfeit identification documents and credentials on the Internet and the criminal uses to which such phony documents can be put. Over the last five months, Subcommittee staff have devoted hundreds of hours to surfing the Internet as part of an effort to understand this little known but growing cadre of Web sites that offer fake identification materials. In furtherance of the investigation, the Subcommittee issued 11 subpoenas for documents and depositions and interviewed over 40 witnesses. My testimony today will provide a brief summary of that investigation and its findings.

The Subcommittee staff began this inquiry by using Internet search engines to develop a list of Web sites that offer fake identification documents. After reviewing over sixty Web sites, we focused our investigative efforts on fifteen sites that purported to sell fraudulent identification documents or the means for customers to create the documents themselves. The Subcommittee staff then commenced an undercover operation in which we ordered - using the fictitious name "Keith Wilson" - products offered by several of these Web sites. Through these undercover purchases the Subcommittee acquired several high quality, false identification products, including a counterfeit driver's license for the State of Oklahoma, templates that could be used to produce fake driver's licenses from numerous states, authentic-looking birth certificates, and documents that could be used to fabricate credentials for employment.

Based upon this undercover operation and information obtained from the Web sites of these companies, the Subcommittee staff narrowed its focus to three major operators of sites that manufacture and/or market phony IDs. The first site is [fakeid.net](http://fakeid.net), which is operated by Brett Carreras, a twenty-one year old student at Loyola University in Baltimore, Maryland. Mr. Carreras started his site on July 28, 1998.

His site offers top quality templates, or computer files, that allow customers to manufacture their own fake identification documents. For instance, [Refer to Ex. 4], this is a file from Mr. Carreras'

site that depicts a template for a previous version of a driver's license from the State of Maine. We found that someone with a computer can use this template to manufacture a counterfeit license that is of very high quality. [Refer to Ex. 5] Indeed, at my request, Subcommittee staff used Mr. Carreras' template to create this fake Maine driver's license bearing my picture, and did so in only a few minutes.

In return for computer access to these templates, Mr. Carreras charged his customers a monthly fee of \$14.95. Billing records obtained by the Subcommittee indicate that, in the two months between mid-October 1999 and mid-December 1999, Mr. Carreras received 621 orders and generated over \$8,000 in sales revenue. Earlier this year, Mr. Carreras announced that he intended to open two more Web sites called [illegalimmigrant.com](http://illegalimmigrant.com) and [fake-id.com](http://fake-id.com). Mr. Carreras advertised [illegalimmigrant.com](http://illegalimmigrant.com) as a site that would specialize in "identity documents such as passports, social security cards, green cards, SSN lists, generators . . . resident alien cards, birth certificates . . . and many more!"

The Subcommittee staff was unable to obtain additional information about Mr. Carreras and his Web sites because he declined to respond to the Subcommittee's interrogatories after invoking his Fifth Amendment right against self-incrimination. Mr. Carreras also refused to answer any substantive questions at a Subcommittee deposition on the grounds of his Fifth Amendment rights.

The second site is [fakeidzone.com](http://fakeidzone.com), which began operations on October 2, 1998. It is operated by Tim Catron, who resides in Lawrence, Kansas. Mr. Catron sells a computer disk that includes templates for various types of fraudulent identification documents. Mr. Catron charges from \$19.95 to \$39.95 for the disk. Billing records obtained by the Subcommittee indicate that, over a two month period in late 1999, Mr. Catron received 652 orders and generated revenue of over \$12,000.

[Refer to Ex. 6] As this page from Mr. Catron's site indicates, the disk contains a Fake ID Kit that includes "college transcripts you customize, college diplomas, new birth certificates, green cards, social security cards, updated driver's license, plus more." The site adds that "[w]e provide you with templates and step by step instructions on what you need to create fake ids so real you could fool your own mother." As with Mr. Carreras, Mr. Catron refused to give deposition testimony to the Subcommittee after invoking his Fifth Amendment right against self-incrimination.

The third site is [bestfakeids.com](http://bestfakeids.com), which is operated by Tim Beachum, a resident of Virginia Beach, Virginia. According to the deposition testimony of Mr. Beachum, he purchased the materials for his site from Mr. Catron and began operations on May 25, 1999. Mr. Beachum charges \$39.97 for essentially the same Fake ID Kit that is sold by Mr. Catron. Mr. Beachum estimates that, in the one year that his site has been operational, he has sold over 1,100 kits and earned almost \$28,000 from the site.

Not only does Mr. Beachum's site offer driver's licenses, but he sells a birth certificate from an actual hospital in Waukegan, Illinois. During his deposition, Mr. Beachum claimed that he modified the birth certificate so that it would be distinguishable from the real certificate issued

by the hospital. Subcommittee staff contacted Victory Memorial Hospital, however, and obtained a copy of a birth certificate that it issued prior to 1990. [Refer to Ex. 7] As this exhibit shows, the phony birth certificate sold by Mr. Beachum is virtually identical to the authentic birth certificate that the hospital formerly used. Mr. Beachum also sold fake press passes that he promoted with fictitious testimonials from individuals who had purportedly used the credentials to gain access to restricted events, such as concerts.

The Internet offers many exciting opportunities for commerce but, as our investigation has shown, it can also offer inventive criminals more effective tools to engage in illegal conduct. After reviewing the activities and products of these Web sites, we believe that several general findings can be made. First, many Internet sites offer a wide variety of phony identification documents, and some of these sites offer extremely high quality counterfeits that include security features, such as holograms, designed to make the documents appear authentic. In fact, most of these sites market their products by touting the ability of the fraudulent IDs to pass as authentic.

Second, this marketing strategy is inconsistent with the disclaimers posted on some Web sites, which claim that the phony IDs are for "novelty" purposes only. For instance, [Refer to Ex. 8] Mr. Beachum's site offers these two Activity Coordinator certificates which were supposedly issued by Kent State University and the Ohio Health Care Association. At his Subcommittee deposition, Mr. Beachum testified that he never intended for his customers to use the certificates to get a job. Indeed, his site includes a disclaimer that states, "[a]ll information on this Web site is for entertainment and educational purposes only." However, Mr. Beachum's marketing shows that he expects and encourages his customers to pass-off his phony documents as legitimate credentials.

His Web site states as follows: "Receive access to authentic downloadable certification certificates to get you a job as an Activity Coordinator. Why should you pay a thousand dollars for a couple of certificates just to learn how to plan activities for individuals." And, just in case the customer isn't sure how to use these fraudulent documents, Mr. Beachum gives them some helpful hints: "We have received tons of e-mails from people wanting documents that could help them get jobs . . . When you use the following certificates to apply for a job you should use them together. On the first blank line place your full birth name. On the last line place the date that the certificate was issued, make sure that the date is the same on both certificates." We do not know whether anyone has used these certificates, but we do know that Mr. Beachum sold them for that purpose. His marketing vividly illustrates how many of these sites attempt to shield themselves from criminal liability through the use of disclaimers that are patently disingenuous efforts to mask their intent to sell illegal products.

We found that these Web site operators are quite ingenious in their efforts to evade the law. [Refer to Ex. 9] This is a counterfeit driver's license for the State of Oklahoma that we purchased undercover from a Web site known as [theidshop.com](http://theidshop.com). With your permission Chairman Collins, I would like to enter this fake license into the hearing record and submit it to the Subcommittee for inspection.

As required by federal law, the document appears to have the words "NOT A GOVERNMENT DOCUMENT" printed diagonally in red ink across the front and back. But, as you can see, this disclaimer is easily removed by cutting the top portion of the lamination and removing the actual identification document. [Refer to Ex. 10] There are even message boards, like this one, that instruct customers how to remove the disclaimer: "Ok, the IDShop sends their ID in a white envelope, exactly as they describe on their webpage. When you open this envelope, the ID has a laminated wrap, extending well over the edge of the ID. It also has printed, NOT A GOVERNMENT DOCUMENT, printed across the lamination in Red. This slip is easy to remove with scissors, and takes less than a minute."

Incidentally, this site is operated by a young man named Robert Sek, who recently had his operation shut down by the Secret Service and Texas authorities. Law enforcement authorities seized from his apartment a computer, photographic quality printer, ID making machine, printed identification cards, and a safe containing holograms and approximately \$25,000 in cash. Pending the criminal investigation, Mr. Sek refused - through his counsel - to discuss his activities with Subcommittee staff.

Our third finding is that the Internet has greatly facilitated the manufacture and sale of counterfeit identification documents by allowing sellers to mass market high quality fake IDs with virtual anonymity. This has, in turn, presented significant obstacles to effective law enforcement. Mr. Catron's Web site illustrates the challenges that these Internet sites present to law enforcement. When he registered his Web site on the Internet, he attempted to disguise the real location of his operation by listing an address and telephone number in the Philippines, and an e-mail address that appeared to originate from another small country in the South Pacific. We eventually discovered that Mr. Catron directed payments to an address in Pittsburg, Kansas. And, we finally obtained Mr. Catron's actual location in Lawrence, Kansas after enlisting the U.S. Marshals Service to serve him with a subpoena. Mr. Catron's tactics, including the use of private mail receiving agencies and multiple anonymous e-mail accounts, allowed him to market his products to a wide audience with very little overhead cost and minimal risk of criminal exposure.

In conclusion, our investigation found that a significant number of Web sites offer a wide range of counterfeit identification documents, and that some of these sites offer phony documents of shockingly high quality. Moreover, we found that the distribution of these counterfeit materials is growing because of the expanding technology of the Internet. This new technology could very well result in a flood of phony identification documents and counterfeit credentials if steps are not taken to curb this emerging problem. It will be no easy task to maintain the integrity of the identification documents on which both the government and the private sector rely.

Chairman Collins, this concludes my prepared remarks. I would be pleased to answer any questions that you and the Subcommittee might have regarding the staff's investigation.