



Intelligence Assessment



(U) Security Threat: Fraudulent Law Enforcement Credentials and Badges

Date 23 November 2010

No. S-027-2010

UNCLASSIFIED//FOR OFFICIAL USE ONLY//
LAW ENFORCEMENT SENSITIVE (U/FOUO/LES)

Prepared by:
Department of the Army Police
Investigations Division / Intelligence Unit
Fort Monmouth, New Jersey

Fraudulent Identity Document Intelligence Group (FIDIG)

WARNING: This document is classified as UNCLASSIFIED//FOR OFFICIAL USE ONLY//LAW ENFORCEMENT SENSITIVE. It contains information that is exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and destroyed in accordance to DoD and Army policy relating to FOUO information and is not to be released to the public, media, or other personnel who do not have a valid need-to-know without prior approval of the drafting agency. State and local homeland security officials may share this document with authorized personnel without further approval from the DoD or Army.

This document is property of the United States Government and is intended for the use of the individual or entity to which it is addressed. Reproduction or release of information contained herein without the permission of the United States Government is prohibited by law, and may subject those responsible for its unauthorized release to criminal and/or civil penalties.

Derived from: Multiple Sources

(U) Security Threat: Fraudulent Law Enforcement Credentials and Badges

(U) Scope Note

(U) This intelligence assessment explores the availability to purchase fraudulent federal law enforcement credentials and badges and how their use is a direct threat to the security of military installations, federal facilities, other critical infrastructure.

(U) Source Summary

(U) Data for this report was obtained from FBI information, DoD information, GAO reports, and open-source documents. Additionally, data was obtained directly from the investigative efforts of the agency publishing the assessment. The reliability of these sources is assessed as HIGH.

(U) Key Questions

(U) How easily and inexpensively can high quality fraudulent badges and credentials be obtained by individuals who threaten the security of the United States?

(U) In regards to access to our military installations, federal facilities and other critical infrastructure, to what extent do we challenge the identification of individuals displaying law enforcement credentials?

(U) What forms of secondary identification are available to assist personnel in verifying the legitimacy and an individual displaying law enforcement credentials?

(U) Key Assumptions

(U) Terrorists will continue to plot attacks against military installations, federal facilities and other critical infrastructure.

(U) Attacks against installations and facilities can be facilitated by individuals using fraudulent law enforcement badges and credentials to gain access as part of their surveillance, planning and attack phases of their operation.

(U) Introduction

(U) The law enforcement badge is a symbol of authority that traces back to medieval times, when the sitting king would grant coats of arms and heraldic shields to those who served the kingdom of his court. Coats of arms were usually found on shields, and these symbol indicated official recognition by the ruler of the land. It conveyed that the bearer of the shield had the authority to display it in the name of the king. Law enforcement badges and credentials started being utilized in the United States with the formation of some of the earliest federal law enforcement agencies such as the United States Marshals Service and the Postal Inspection Service.

(U) Today, badges convey that the bearer is granted the authority to enforce laws established by a governmental or quasi-governmental entity and are cherished by law enforcement officers. The issue is that there are over 17,000 law enforcement agencies in the United States all with different badges and credentials issued to their personnel. This is not including, the over 70 different federal law enforcement agencies that issue badges and/or credentials. And in there lies the problem. How do you know a cop is a cop?

(U) The most common response to that question is usually, if they walk like a cop. Talk like a cop. And look like a cop, then they are a cop. The assumption is further built upon when being presented with a badge and identification card. But that is not always the case.

(U) In 2008, Bill A. Jakob was arrested for impersonating a federal agent in the town of Gerald, Missouri. Jakob came to town offering the federal government's assistance in combating the town's growing methamphetamine problem. Together with local police, Jakob conducted investigations, conducted searches and seizures and arrested offenders all under the cloak of being a federal drug agent. However, Jakob was not a federal agent but an unemployed trucking company owner.

(U) Jakob certainly looked the part. His hair was cut short and he sometimes wore a t-shirt that read "Police". He wore military style clothing, carried a badge and drove a Ford Crown Victoria fitted with police radios and flashing emergency lights. Jakob was able to fool an entire local police department, the town's mayor and other government officials.

(U) Fraudulent badges and credentials are easily obtained via the internet and are generally of such high quality that a law enforcement officer carrying the same badge could not tell the difference between them.

(U) Obtaining Fraudulent Federal Law Enforcement Badges

(U/FOUO/LES) Between November 2009 and March 2010, undercover investigators were able to purchase nearly perfect counterfeit badges for all of the Department of Defense's military criminal investigative organizations to include the Army Criminal Investigation Command (Army CID), Naval Criminal Investigative Service (NCIS), Air Force Office of Special Investigations (AFOSI), and the Marine Corps Criminal Investigation Division (USMC CID). Also, purchased was the badge for the Defense Criminal Investigative Service (DCIS) [See Figure 1].

(U/FOUO/LES) Also available for purchase were counterfeit badges of 42 other federal law enforcement agencies including the Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), Alcohol, Tobacco and Firearms (ATF), Secret Service, and the US Marshals Service.

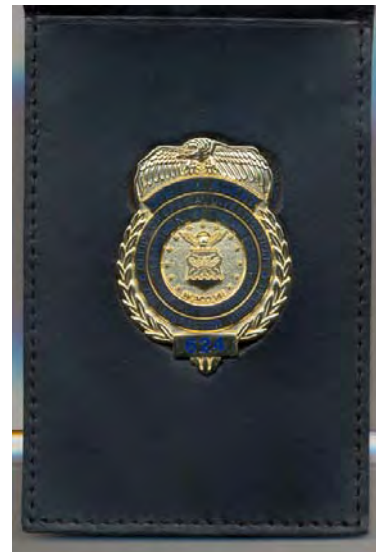


Figure 1. Air Force OSI Badge and Case

(U/FOUO/LES) Of the other federal law enforcement agency badges available, the investigators found exact reproductions of the badges issued to Federal Air Marshals, Transportation Security Administration (TSA) Screeners, TSA Inspectors, and Special Agents of the TSA Office of Inspector General.

(U/FOUO/LES) These purchases were made from three internet sites operating in Germany, United Kingdom, and Bucharest, as well as from individuals on several internet auction sites [See Appendix 1, 2, and 3]. The only question asked by the sellers during the transaction was, "Are you a collector?" With an affirmative response, the badges were then mailed to a Post Office Box address in the United States.

(U/FOUO/LES) On two occasions, investigators purchased a FBI and DEA Special Agent badge directly off of the auction site eBay, in direct violation of eBay's policies prohibiting the sale of such items on the site [See Appendix 4]

(U/FOUO/LES) The average cost of a badge was \$60 USD. Through numerous email communications with the vendors, investigators were able to make purchase arrangements to acquire badges in bulk (50 units and above) where the price per unit was dropped as much as 75%.

(U/FOUO/LES) All of the internet sites in question, referenced the fact that possession of federal law enforcement badges in the United States is illegal and that purchasers should consult their local laws before ordering. While this disclaimer was posted on the site, the investigators had no problems making a purchase and having it mailed to the United States.

(U/FOUO/LES) Utilizing the services of Alexa Internet Research, an analysis was conducted of the three internet sites that were utilized to make purchases. While these vendors (sites) are located in Germany, United Kingdom and Bucharest, over 60% of visitors to these sites are utilizing IP addresses located in the United States.

(U) Obtaining Fraudulent Federal Law Enforcement Credentials

(U/FOUO/LES) Investigators obtained fraudulent law enforcement credentials via two methods. The first method was investigators creating their own utilizing information downloaded from the internet, commercially available software, ink jet color printers and lamination. The credentials created did not look anything similar to the genuine law enforcement issued by the agencies.

(U/FOUO/LES) While conducting research on the internet to create the credentials, investigators did located scanned images of FBI, DEA and Federal Air Marshals credentials belonging to former agent. Some had posted the images on internet pages for their post-federal employment in the private investigations and security industry. Additionally, investigators located an internet site in Spain that offered for sale reproductions of the current identification cards issued by the New York City and Los Angeles Police Departments.

(U/FOUO/LES) The second method utilized by investigators was to purchase blank federal law enforcement credentials from individuals offering them for sale. Undercover investigators were

able to locate a USPER counterfeiter operating in Hoboken, New Jersey that offered to sell computer templates to create FBI, DEA, ATF, Naval Intelligence, NASA, and NYPD credentials. The counterfeit ATF and NYPD credentials were so close to the genuine that some personnel could not readily identify the genuine from the counterfeit when placed next to each other [See Appendix 5].

(U/FOUO/LES) In order to use the counterfeit badges and credentials, investigators needed to obtain a badge and credential case similar to those used by federal agents. Numerous vendors were located on the internet that supplied custom badge and credential cases to the general public. While selecting one of these vendors would have certainly been the easiest course of action, investigators wanted to see if they could obtain the actual badge and credential cases issued to certain federal law enforcement agencies. The investigators contacted the vendors and with little effort, had several badge and credential cases mailed to a Post Office Box with no questions asked as to why they were being mailed to an individual rather than an agency.



Figure 2. Army Criminal Investigation Command Badge and Case

(U/FOUO/LES) Also, the vendors from which the counterfeit badges were purchases from did offer leather credential cases customized with imprinted lettering for several agencies such as Army CID, NCIS, US Marshals Service and the FBI [See Figure 2].

(U) Testing Security at Federal Facilities Utilizing Fraudulent Federal Law Enforcement Badges and Credentials

(U) In a report published in May of 2000, the U.S. General Accountability Office (GAO) detailed the results of an undercover investigation where federal investigators utilized fraudulent law enforcement badges and credentials to penetrate the security at federal buildings and airports. The investigation found that investigators were 100% successful in penetrating 19 federal sites and 2 commercial airports by claiming to be law enforcement officers and entering the facilities unchecked by security where they could have carried weapons, listening devices, explosives, chemical/biological agents and other such materials.

(U/FOUO/LES) Over 10 years later, Army investigators were able to duplicate the findings of the GAO's investigation with 100% success. During the period of January to June 2010, undercover investigators utilized fraudulent badges and credentials of the DoD's military criminal investigative organizations to penetrate the security at: 6 military installations; 2 federal courthouses; and 3 state buildings in the New York and New Jersey area.

(U/FOUO/LES) On each occasion, the investigators identified themselves as law enforcement officers; displayed both a fraudulent badge and credentials; and stated that they were armed. In instances where a magnetometer was being utilized they were waved through without being screened after identifying themselves as federal law enforcement [See Figure 3].

(U/FOUO/LES) Once being granted access to the military installation or federal facility, the investigators proceeded to areas that were designed as “Restricted Area” or “Authorized Personnel Only” and were able to wander around without being challenged by employees or security personnel. On one military installation, investigators were able to go to the police station and request local background checks on several fictitious names. All that was required was displaying the fraudulent badge and credentials to a police officer working the communications desk.

(U/FOUO/LES) In preparation for the operation, investigators conducted internet research to determine if certain military installations and federal facilities had posted access control policies available for public view. The research found at least 12 military installations through the US have published their access control policies online for public view. After reviewing the policies, investigators found consistently, producing federal law enforcement credentials to security personnel allow for unescorted access to the installations.



Figure 3. Example of Air Force OSI credentials used during one of the security tests.

(U/FOUO/LES) Although security has increased since 9/11, access to military installations and federal buildings can be obtained by individuals who appear to belong. Those that can “walk the walk” and “talk the talk” while producing fraudulent credentials. Allowing an armed individual entry into these types of facilities can have a disastrous effect. The ability to conduct a small arms attack; plant explosive devices; release biological or chemical agents; and murder a judge or witness all come into play.

(U) Ten years after the GAO’s investigation highlighted the security risks with using fraudulent law enforcement identification, security procedures have not changed. By examining how access to our critical assets and infrastructure can be compromised and security checks points almost eliminated by individuals using fraudulent law enforcement credentials, government stakeholders must develop security plans that address these issues. While conducting the security tests the investigators did not however, that some of the fraudulent badges used were of such high quality that a reasonable person would not be able to tell the difference between a genuine and counterfeit.

(U) Alternate Forms of Identification to Confirm Government Affiliation

(U) In August of 2004, President George W. Bush issued Homeland Security Presidential Directive 12 (HSPD-12) which mandated new standards for secure and reliable personal identification for all federal employees and contractors, including federal law enforcement personnel. These identification cards are referred to as Personal Identity Verification (PIV) cards and are designed to be resistant to identity fraud, tampering, counterfeiting and terrorist exploitation. The DoD calls their version of the PIV card, the Common Access Card (CAC) [See Figure 4].

(U) The header of the PIV card says “United States Government” and includes some of the following standardized features: (1) Printed picture of your face; (2) Agency seal; (3) Agency affiliation; (4) Organization affiliation; (5) Card expiration date; and (6) Card serial number. The card will also contain an integrated circuit chip which is clearly visible on the front. Those federal employees who as designated as an “Emergency Response Official” will have a red box containing that phrase at the bottom of the card.

(U) While each federal law enforcement agency issues different credentials and badges to their officers and agents, these personnel should still also possess a PIV or CAC card which can be used as a secondary form of identification to verify the legitimacy of individual claiming law enforcement authority or government affiliation.

(U) Several state law enforcement certification boards have also elected to issue a standardized identification card to peace officers indicating, among other things, that they are a certified peace officer. These identification cards are issued in addition to the unique identification or credentials issued by an individual law enforcement agency and can be used as a secondary form of identification.

(U) One example of this standardized issuance is the identification card (PID) issued by the Colorado Peace Officer Standards and Training Board (POST). The Colorado POST issues a PID card to every certified peace officer in the state. The PID cards are designed to provide each officer with a standardized identification, a unique identification number, and a electronic method for the Colorado POST to track and officer’s attendance in training courses.



Figure 4. Example of DoD Common Access Card and Personal Identity Verification Card

(U) Analysis of Terrorist Attack Phases

(U/FOUO/LES) Terrorists, including the 9/11 attackers, had used fraudulent documents during the various phases of planning and attacks.

(U) Terrorist Attack Phases:

- (U) Initial Target Selection
- (U) Initial Surveillance
- (U) Final Target Selection
- (U) Pre-attack Planning
- (U) Final Surveillance
- (U) Deployment of Attack Team
- (U) Attack

(U/FOUO/LES) Analysis of the seven phases of the Terrorist Planning Cycle reveals several weaknesses in our current security operations. The use of these fraudulent credentials would enable terrorists to reduce their expenditure of funds, resources and manpower. This weakness would also allow for long term chemical or biological attacks as well as short term IED, VBIED and small arms attacks against military installations and other federal facilities. This weakness allows a terrorist group to initiate an attack at any phase within the cycle.

(U) Improving Recognition and Identification of Fraudulent Badges and Credentials

(U/FOUO/LES) Due to large number of various federal, state, and local law enforcement credentials this becomes a very large task. Law enforcement and security officers must be aware of what appears to be out of place and to challenge individuals and their credentials.

(U) Training of personnel tasked with granting access to installations on how to challenge and verify credentials that are being displayed is essential to prevention.

(U) Understanding how easily these credentials are obtained will assist us in the implementing of protective measures to detect, deter, and defense against future attacks from various terrorist groups.

Questions or comments regarding this intelligence product should be directed to Captain Andrew Poulos, andrew.poulos@us.army.mil or Detective Matthew Sharin, matthew.sharin@us.army.mil.

Appendix 1
Analysis of My Badges

Common Name: **My Badges**

Internet Address: <http://www.my-badges.com> / <http://www.badge-police.com>

Online Since: **January 3, 2010**

Server Location: **Bucharest**

Number of Hits Per Month: **Unknown**

Number of Hits Per Month by U.S. Users: **Unknown**

Software: N/A

Description (from internet site):

Internet auction site, similar to eBay, that offers U.S. federal, state and local law enforcement badges for auction. Bidders must register for an account prior to submitting a bid. Majority of purchases are completed via PayPal money transfers. Costs range from \$55 to \$275.

U.S. Federal Law Enforcement Badges For-Sale:

DEA (Special Agent)
DEA (Task Force Officer)
FBI (Special Agent)
Secret Service (Special Agent)
Secret Service (Technician)
Secret Service (Uniformed Division)
Pentagon Police (Officer)
DCIS (Special Agent)
Army CID (CID Agent)
Air Force OSI (Special Agent)
US Marine Corps CID (CID Agent)
NCIS (Special Agent)
ATF (Special Agent)
Postal Inspection Service (Postal Inspector)
EPA CID (Special Agent)
ICE (Special Agent)
ICE (Officer)
TSA (Federal Air Marshal)
US Marshal Service (Deputy U.S. Marshal)
US Marshal Service (Special Deputy U.S. Marshal)
US Marshal Service (Supervisory Deputy U.S. Marshal)
Diplomatic Security Service (Special Agent)
IRS CID (Special Agent)
NASA OIG (Special Agent)
National Security Agency (Special Agent)
CIA Protective Operations Division (Special Agent)



Picture from Website



Picture from Website

Appendix 2
Analysis of Police Badge Store

Common Name: **Police Badge Store**
Internet Address: <http://www.policebadgestore.co.uk>
Online Since: **August 11, 2009**
Server Location: **United Kingdom**
Number of Hits Per Month: **Unknown**
Number of Hits Per Month by U.S. Users: **Unknown**
Software: N/A

Description:

Company offers for sale counterfeit/reproduced U.S. federal law enforcement badges. The website states that badges will only be sold to collectors and makes mention to certain federal statutes in the United States related to the possession of such reproduced badges. Costs range from \$55 to \$500.

U.S. Federal Law Enforcement Badges For-Sale:

DEA (Special Agent)
DEA (Task Force Officer)
FBI (Special Agent)
Secret Service (Special Agent)
Secret Service (Technician)
DCIS (Special Agent)
Army CID (CID Agent)
Air Force OSI (Special Agent)
US Marine Corps CID (CID Agent)
NCIS (Special Agent)
ATF (Special Agent)
Postal Inspection Service (Postal Inspector)
EPA CID (Special Agent)
ICE (Special Agent)
ICE (Officer)
CBP (Officer)
CBP (Border Patrol)
TSA (Officer)
TSA (Federal Air Marshal)
US Marshal Service (Deputy U.S. Marshal)
US Marshal Service (Special Deputy U.S. Marshal)
US Marshal Service (Supervisory Deputy U.S. Marshal)
Diplomatic Security Service (Special Agent)
IRS CID (Special Agent)
NASA OIG (Special Agent)
National Security Agency (Special Agent)
U.S. Park Police
Bureau of Engraving and Printing Police



Picture from Website



Picture from Website

Appendix 3
Analysis of Shield Badges

Common Name: **Shield Badges**

Internet Address: <http://www.policebadge.org>

Online Since: **July 2006**

Server Location: **Germany**

Number of Hits Per Month: **Unknown**

Number of Hits Per Month by U.S. Users: **Unknown**

Software: N/A

Description:

Company offers for sale counterfeit/reproduced U.S. federal law enforcement badges. The website states that badges will only be sold to collectors and makes mention to certain federal statutes in the United States related to the possession of such reproduced badges. Costs range from \$55 to \$275.

U.S. Federal Law Enforcement Badges For-Sale:

DEA (Special Agent)

DEA (Task Force Officer)

FBI (Special Agent)

Secret Service (Uniformed Division)

Army CID (CID Agent)

Air Force OSI (Special Agent)

US Marine Corps CID (CID Agent)

NCIS (Special Agent)

ATF (Special Agent)

ICE (Special Agent)

US Marshal Service (Deputy U.S. Marshal)

Diplomatic Security Service (Special Agent)

NASA OIG (Special Agent)



Picture from Website



Picture from Website



Picture from Website

Appendix 4 eBay Prohibited Items

Government documents, IDs, and licenses policy

To prevent false identities, comply with the law, and help ensure public safety, we don't allow government identification cards, such as driver's licenses and passports to be offered for sale of eBay.

Federal regulations also prohibit the sale of classified government documents (internal paperwork) that are not for public use) and certain types of government-issue medals, so such items can't be sold on eBay. For more examples of government related items that aren't allowed, see the guidelines below.

ALLOWED:

- Antique (generally more than 100 years old) government documents such as birth certificates, marriage licenses, and ship captain's licenses.
- Expired U.S. passports that were issued more than 20 years prior to the date of the sale.
- Services for obtaining a license.

RESTRICTED:

- Collectible vehicle license plates that are a least 3 years old. Sellers need to clearly state the plate's age in their listing description.
- Novelty certificates, as long as the listing specifies that it's a novelty item.

NOT ALLOWED:

- AutoCheck or Carfax reports.
- Birth Certificates or a completed applications for a birth certificate.
- Classified or restricted government documents.
- Current vehicle license plates and plates that look like current license plates.
- Documents that are designed to look like official documents but are actually fake.
- Driver's licenses or completed applications for a driver's license.
- Fake certificates or diplomas.
- Fake IDs such as licenses or passports.
- Government vehicle license plates.
- Government issued medals and certificates for medals include the Air Force Cross, Congressional Medal of Honor, Distinguished Service Cross, Navy Cross, Purple Heart, or Silver Star. This also applies to a medal's associated buttons, ribbons, or rosettes.
- Items that are used to create or modify IDs, government documents, licenses, or plates.
- Passports or a completed application for a passport.
- Vehicle Identification Number (VIN) plates.
- VIN plate rivets.
- Vehicle titles or vehicle title stocks (although a vehicle title that's being sold with a vehicle is OK)

Police-related items policy

With some exception, we generally don't allow listings for law enforcement badges or official law enforcement equipment from any public entity. This includes badges issued by the government or any country. This rule also applies to police badges and official equipment from federal, state, or local law enforcement agencies in the U.S.

Make sure your listing follows these guidelines. If it doesn't, it may be removed, and you may be subject to a range of other actions, including restrictions of your buying and selling privileges and suspension of your account.

ALLOWED:

- Fake, novelty, or clearly unofficial badges such as plastic or cartoon badges.

RESTRICTED:

- Badges that meet both of these requirements:

The issuing law enforcement organization has authorized in writing that the item can be sold; and a copy of the authorization letter with the law enforcement contact (name and phone number) is included in the listing.

- Historical badges that meet both of these requirements:

The listing description clearly states that the badge is a historical piece that's at least 75 years old or was issued by an organization that no longer exists; and the item doesn't look like a current-issue law enforcement badge (for example, an antique sheriff's badge from 19th century Tombstone). If we have reason to believe that the item looks like a current-issue badge, we may remove the listing for public safety reasons.

- Mini-badges that are about 1 inch by 1 inch in size. The listing has to include a picture of the items that shows scale.

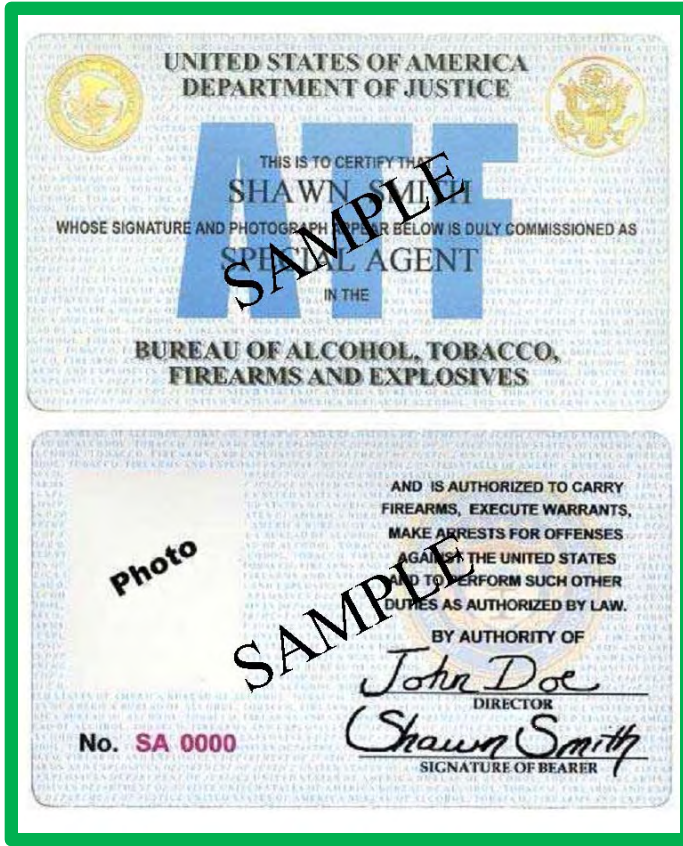
NOT ALLOWED:

- Badges encased in Lucite.
- Badges from federal law enforcement agencies including:
 - Bureau of Indian Affairs
 - Central Intelligence Agency (CIA)
 - Federal Bureau of Investigation (FBI)
 - Military Police (MP) or Criminal Investigative Services
 - Transportation Security Administration (TSA)
 - U.S. Immigration and Customs Enforcement
 - U.S. National Park or Forest Service
 - U.S. Marshal
 - U.S. or Canadian Border Patrol
 - U.S. Postal Inspector
 - U.S. Secret Service

- Badges from state, county, or other municipal law enforcement agencies.
- Badges issued by foreign government
- Badges issued by private security companies
- Badges, patches or patches in the shape of a badge
- Credential cases
- Identification cards or credentials for members of law enforcement
- Mini TSA badges
- Movie prop badges
- Private Investigator badges
- Quasi-law enforcement badges such as fire department badges
- Reproduction of current police badges, including fake badges that look like current police badges – for example, an X-Files FBI badge
- Special Event badges like inauguration badges

Source: eBay website, <http://pages.ebay.com/help/policies>

Appendix 5
Genuine vs. Counterfeit Credentials



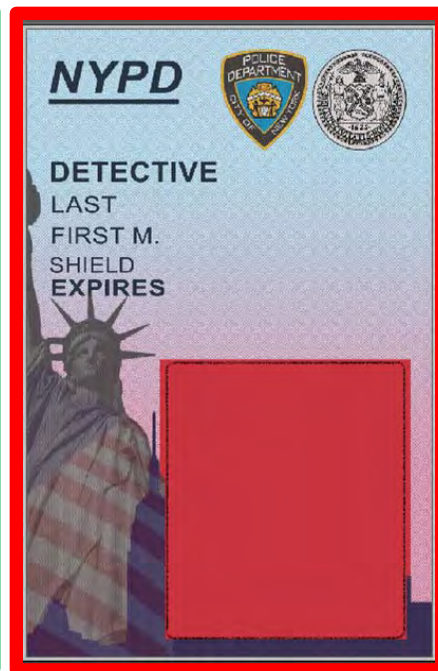
GENUINE



COUNTERFEIT



GENUINE



COUNTERFEIT