COUNTERFEITING OF DRIVER'S LICENSES

An increasing threat to the United States and what to do about it

DSA

ENHANCING DOCUMENT AND IDENTITY SECURITY

COUNTERFEIT DRIVER'S LICENSES: AN INCREASING THREAT

EXECUTIVE SUMMARY

The counterfeiting of state-issued driver's licenses (i) presents an imminent threat to national security, (ii) causes colossal financial losses for state and federal governments, and (iii) enables substantial increases in identity theft and fraud losses to businesses, banks, and private citizens.

Counterfeiting thrives at multiple levels and the use of counterfeit driver's licenses is a major contributor to the staggering costs borne by our society.[1] Federal, state, and municipal governments collectively lose billions of dollars every year to fraud,[2] a significant portion of which is enabled by counterfeit driver's licenses.

Severe cost constraints are placed on the budgets of driver's license agencies. This results in (i) a critical delay to upgrade the driver's license design – which should occur every four or five years to stay ahead of counterfeiters and reduce the circulation validity of each design – and (ii) an inability to incorporate the latest overt, covert, and forensic security features due to marginal cost considerations. The consequence is that high-quality counterfeit state driver's licenses can be readily purchased from internet sites fronting for criminal organizations.

TABLE OF CONTENTS

EXECUTIVE SUMMARY | PAGE 2

COUNTERFEITING: A GROWING THREAT | PAGE 4

COUNTERFEITING'S REAL COST TO GOVERNMENTS AND CITIZENS | PAGE 4

HOW COUNTERFEITING THRIVES | PAGE 4

BEATING BACK COUNTERFEITERS: BEST PRACTICES | PAGE 5

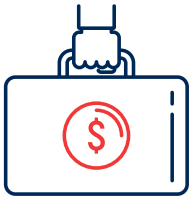
CONCLUSION | PAGE 6

ADVANCED SECURITY FEATURES FOR DRIVER'S LICENSES | PAGE 7

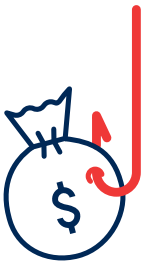
REFERENCES | PAGE 8

COUNTERFEIT DRIVER'S LICENSES ARE USED TO:

establish false identities



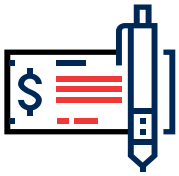
facilitate white collar & organized crime



conduct online financial fraud

support hijacking of shipments

establish shell companies & accounts



enable physical check fraud

COUNTERFEIT DRIVER'S LICENSES: AN INCREASING THREAT

State governments must understand the significant downstream costs to their taxpaying citizens due to issuing driver's licenses that are easily counterfeited. By investing more in the security of their driver's license, states would be rewarded with lower fraud losses and fewer identity-related crimes. To effectively combat the growing threats associated with counterfeit licenses, it is recommended that state legislatures allocate appropriate funding to arm states with the necessary resources to increase their card security requirements. Doing so will provide their citizens with driver's licenses that have vastly improved security and resistance to counterfeiting.

COUNTERFEITING OF DRIVER'S LICENSES CONTRIBUTES TO ANNUAL COSTS ASSOCIATED WITH:

$61.9 B
underaged drinking

$174 B
counterterrorism

$13 B
traditional identity fraud

$4.1 B
check and bank fraud

$9.7 B
returned goods

Totaling more than $250 billion, these equate to an annual cost of $1,000 for every adult in the United States.

ABOUT DSA

DSA is a globally recognized organization focused on advancing existing and emerging security document and mobile identity solutions.

DSA is committed to identifying threats to legitimately issued identification documents, mobile identification, banknotes, document production, and issuance processes.

Our approach embodies two key principles:

- Ensuring that sufficient levels of security and supporting systems are adopted to establish the optimal protection for each application.
- Improving the protection and security of our institutions and citizens while complying with governing laws and safeguarding social liberties.

DSA membership encompasses the leading document security and identity experts from the public and private sectors. Members provide extensive technical and practical expertise, which we incorporate into every aspect of our organization.

Governments rely on DSA for guidance and support when upgrading their security documents and identity strategies.

DSA
ENHANCING DOCUMENT AND IDENTITY SECURITY

documentsecurityalliance.org

COUNTERFEIT DRIVER'S LICENSES: AN INCREASING THREAT

COUNTERFEITING: A GROWING THREAT

Hundreds of thousands of counterfeit driver's licenses are presented for proof of identity or age verification to businesses across the United States every day. Such counterfeits, amongst other things are used to:

- Facilitate the underage purchase of alcohol
- Deceive banks and retail stores for financial fraud and scams
- Board airplanes, and
- Access secure areas

The massive scale of counterfeit driver's license sales presents a direct threat to public safety, homeland security, and economic stability.

A counterfeit driver's license can serve as a "breeder" document for establishing a false identity. False identities can facilitate a variety of crimes, including money laundering and check fraud, while concealing a criminal that may already be sought by law enforcement. A well-documented fictitious identity provides an opportunity for terrorists to move freely within the United States without triggering name-based watch lists accessed by law enforcement at the federal, state, and local levels. It also allows them to conduct nefarious activities without revealing their true identity. All of these threats are in addition to the anonymous transfer of funds supporting terrorism activities.

The crime of identity theft ranks much higher than does counterfeit currency in terms of the impact on both businesses and average citizens. Personalized identity theft is often done by criminal actors operating in local communities, often as the result of a phone scam or an automobile burglary. The key tools empowering professional identity thieves and fraudsters are counterfeit driver's licenses.[3]

Counterfeiters have become increasingly sophisticated and are able to replicate many of the driver's licenses that are not using state-of-the-art security features.

COUNTERFEITING'S REAL COST TO GOVERNMENTS AND CITIZENS

Annual costs associated with underage drinking ($61.9 billion),[4] traditional identity fraud ($13 billion),[5] receiptless return fraud ($9.7 billion),[6] counterterrorism ($174 billion),[7] check fraud ($1.3 billion),[8] and bank fraud ($2.8 billion)[9] total more than $250 billion dollars. Counterfeit driver's licenses enable these criminal activities. This equates to an annual cost of $1,200 for every adult in the United States.

The total societal cost resulting from underage drinking includes medical spending, property damage, work losses, and other resource expenditures due to harmful behaviors attributed to underage use of alcohol.[10] The National Institute on Alcohol Abuse and Alcoholism stated, "The consequences of underage drinking can affect everyone—regardless of age or drinking status. Either directly or indirectly, we all feel the effects of the aggressive behavior, property damage, injuries, violence, and deaths that can result from underage drinking. This is not simply a problem for some families—it is a nationwide concern."[11] Counterfeit driver's licenses facilitate this behavior.

In 2020, the Federal Trade Commission (FTC) received more than 1.3 million reports from individuals claiming their identity was stolen.[12] Total identity fraud losses in the U.S reached $16.9 billion in 2019, an increase of 13% year-over-year from $14.9 billion in 2018.[13] Counterfeit driver's licenses are a primary tool for the fraudsters.

Retail businesses lose billions of dollars annually due to return fraud, where criminals return stolen goods by using counterfeit driver's licenses as identity.[14] While cashiers are trained to decline transactions if the presented license looks altered or counterfeit, the high quality of many counterfeit driver's licenses makes them very difficult to discern from the legitimate ones.

Since the terrorist events of September 11, 2001, that were facilitated by the use of counterfeit and fraudulently obtained driver's licenses, the United States has spent nearly $3 trillion dollars on counterterrorism.[15] In 2020 alone, counterterrorism spending reached $174 billion.[16] In addition, the federal government spends tens of millions of dollars annually to pursue, arrest, and indict domestic counterfeiters.

COUNTERFEIT DRIVER'S LICENSES: AN INCREASING THREAT

HOW COUNTERFEITING THRIVES

Annually, sales of counterfeit driver's licenses approach $500 million dollars.[17] This illegal market produces counterfeits that enable underage drinking, identity theft and fraud, and terrorism, among a myriad of other criminal activities. Furthermore, profits from this market are often used to fund actions to attack and undermine the United States.[18]

Historically, the production of counterfeit identity documents was limited to a small subset of actors with the skills and tools necessary to produce credible forgeries. Today, low-end counterfeits are not as easily recognizable as they used to be, and high-end counterfeits are excellent. Technological advancements of equipment used by counterfeiters combined with the lack of advanced security features being used in current driver's licenses has made it easier to make convincing counterfeits. There is a much broader market operating in online spaces to sell all types of counterfeit identity documents including passports, driver's licenses, and identity cards. U.S. Customs and Border Protection (CBP) seized 26,250 and 61,679 counterfeit driver's licenses in fiscal years 2019 and 2020 respectively; largely from international packages seized at express consignment facilities (FedEx and UPS).

The demand for counterfeit driver's licenses, mostly purchased via the internet, thrives due to active latent acceptance of counterfeit licenses for proof of age. Counterfeiters have become increasingly sophisticated and are able to replicate many of the driver's licenses that are not using state-of-the-art security features. Because counterfeit driver's licenses are subject to confiscation by responsible alcohol establishments in most states, many counterfeit sites sell them in sets of two. This enables the underage purchaser another opportunity to try to access alcohol if their first attempt is thwarted.

Despite national and state efforts to decrease underage drinking, there is still a high percentage of college students who participate in underage drinking.

There are currently 17.5 million undergraduate students enrolled in colleges nationwide, the majority of whom are under the age of 21.[19] A survey conducted by the Ohio State University newspaper found approximately 69 percent of students had used or owned fake identification, including driver's licenses.[20] A study of three Florida universities published in the American Journal of Public Health Research found that, of the 688 respondents, 273 (33.5%) had a fake ID and the vast majority of these students used fake IDs to purchase alcohol (83.1%) and/or enter a bar to drink alcohol (85.9%).[21]

BEATING BACK COUNTERFEITERS: BEST PRACTICES

Driver's license counterfeiting problems must be addressed by state governments through increased investment in the most advanced security features. Upgrades and advancements in features should focus on ways to combat low-end and high-end counterfeits. Mobile driver's licenses issued as a complementary privacy feature, or for convenience, do not diminish the importance of, or need for, more effort and resources to improve the counterfeit resistance of physical driver's licenses. On the contrary, the physical driver's licenses are often used as a root-of-trust for obtaining a digital credential whether presented on a mobile device or remotely for online transactions. Thus, state governments have no alternative other than to commit more resources to increase the counterfeit resistance of their physical driver's licenses as well as aggressively apprehend and prosecute the users of counterfeit identity documents.

Complex card design

A complex, highly secure document presents significant barriers for counterfeiters. To achieve this, we recommend the protection of the primary photo and other personalized data by deploying multiple security features in a layered approach:

a. Durable polymer card body that that does not allow separation of layers, thereby providing maximum protection of embedded security features

b. High-definition background print designs using secure patterns, guilloche lines, visible and/or invisible luminescent inks, and color-shifting inks to create complex, secure printed cards to prevent digital reproduction/counterfeiting

COUNTERFEIT DRIVER'S LICENSES: AN INCREASING THREAT

c. Embedded security features – including Diffractive Optically Variable Image Devices (DOVIDs) and Optically Variable Devices (OVDs) – with designs that are integrated with the card design, creating a highly complex document that is nearly impossible to counterfeit

d. Incorporation of a contact or contactless integrated circuit chip, as well as machine readable and forensic features to enable the document to be automatically authenticated at the first and second lines of inspection and at forensic laboratories

e. Secure personalization processes that eliminate variations in personalization quality and the potential for insider fraud

Co-existence of physical and digital credentials

As mobile driver's licenses are introduced, they will provide a convenience for individuals who prefer to store their identity on their smart phones. While mobile identity may provide a level of convenience, a portion of the population[22] does not have mobile devices while others are resistant to using them for identity purposes. Of concern with this new technology is the recognition that no digital system is immune to cyber-attacks from individuals, organized crime, and/or overseas state-sponsored organizations. With the threat of such attacks, mobile identity should remain a complement to physical identity – not a replacement.

This combination of mobile driver's licenses and secure physical driver's licenses should be recognized as necessary for a resilient, sustainable, and secure ID system. States must remain vigilant in specifying that their physical driver's licenses be highly secure. Where possible, mobile driver's licenses and physical driver's licenses should be self-referential – each helping to authenticate the other.

Best value vs. low price

Under the REAL ID Act, the Department of Homeland Security stipulated the development of more tamper-resistant driver's licenses with enhanced security features.[23] Unfortunately, the constraints on the budgets of driver's license agencies result in a slower cycle to upgrade the driver's license design. States should update designs every four or five years to stay ahead of counterfeiters. Additionally, since no specific enhanced security features were mandated under REAL ID, states often fail to incorporate the latest overt and forensic security features – security features that are available today but are rarely employed by state driver's license agencies due to marginal cost considerations.

While the lowest bid may seem to be the most attractive, it generally ends up costing governments, and ultimately citizens, far more than the initial contract price as less complex security features make the driver's license easier to counterfeit. Furthermore, low-price contract awards drive innovation out of solutions and cause the low-price approach to trickle down into the supply chain. As an example, many raw materials used in driver's licenses today are not from a secure supply chain and counterfeiters can easily obtain or replicate them.[24]

Evaluation of driver's license solutions should be based on clear requirements that specify the need for high security cards. If the proper technologies or combination of technologies are selected, a more effective solution will be achieved and provide a greater value to the procuring agency. Only anti-counterfeiting technologies that are (i) not easily accessible and (ii) have proven effectiveness against various forms of attack should be specified. Selection should be based on the offer that provides the best combination of high-security and value to the state.

CONCLUSION: WINNING THE FIGHT AGAINST COUNTERFEITING

Beyond the monetary cost of the driver's license, the societal costs of counterfeiting are immeasurable. A single life lost due the sale of a firearm to an individual using a counterfeit identity or, to a drunk underage driver who used a fake driver's license to enter a bar, is too high a price to pay. Financial losses from identity theft and criminal actions are staggering. States need to issue more secure driver's licenses that will result in dramatically lower overall costs.

- **RECOMMENDATION 1**

  State legislatures need to allocate funding to provide state driver's license agencies a larger budget to protect citizen identities through (i) enhanced driver's license card security and (ii) increased enforcement of driver's license fraud and counterfeiting.

COUNTERFEIT DRIVER'S LICENSES: AN INCREASING THREAT

- **RECOMMENDATION 2**

  State transportation and motor vehicle authorities need to increase the card security requirements – beyond the existing minimum standards – for their driver's licenses.

- **RECOMMENDATION 3**

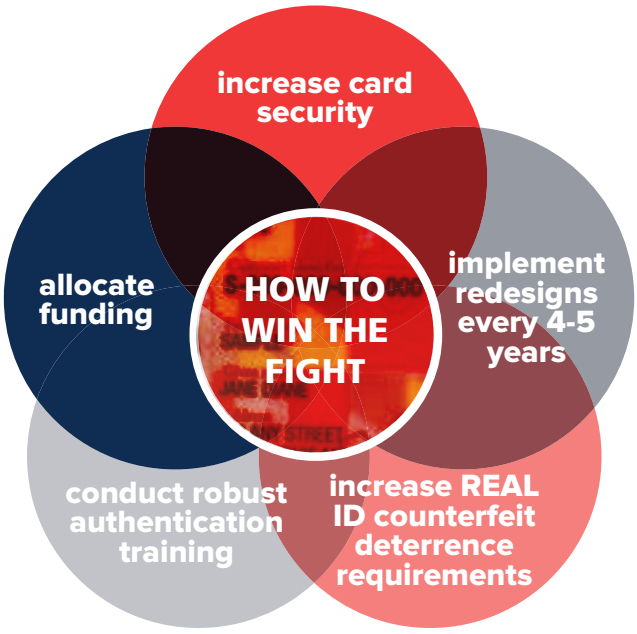
  States need to issue new robust and secure driver's license designs every four to five years, versus the REAL ID minimum requirement of eight years. This matches the five-year procument cycle of many states, reduces the exposure of a given license design to fraud, and reduces the circulation validity of each driver's license design from 16 years to eight to ten years.

- **RECOMMENDATION 4**

  The Department of Homeland Security needs to encourage Congress to update the requirements of the REAL ID Act to increase the counterfeit deterrence requirements of state-issued REAL ID compliant driver's licenses.

- **RECOMMENDATION 5**

  State transportation, motor vehicle and law enforcement authorities need to provide robust authentication training for public and private sector organizations that are responsible for inspection and acceptance of driver's licenses as proof of identity and age verification.



ADVANCED SECURITY FEATURES FOR DRIVER'S LICENSES

Security design and printing

- Fully integrated design coupling multiple security features including printed, embedded, and surface effects into a holistic and secure document.
- High security designs incorporating multiple ink technologies (e.g., security offset, color shifting and UV fluorescence) and security-printed fine-lines and patterns. Printing techniques, such as rainbow guilloche, must be used to remain beyond the skill and equipment of counterfeiters.

Card body substrate

- Polymer substrates that use no adhesive and form a mono-block laminate card structure that is impossible to delaminate without tamper evidence.
- Transparent polymer substrate which contains level one (unaided visual inspection), level two (trained inspection with lights and magnification), and level three (laboratory examination) security features.
- Advanced substrate materials containing color shifting properties.

Card construction

- Windows containing see-through security features or other embedded security features. The windows should be constructed using complex designs, making them extremely difficult to simulate.
- Surface effects such as tactile structures, lenses, or diffractive features that would prevent counterfeiting by over-laminating with fake personalized data.

Embedded security elements

- Security features positioned to protect the primary photograph and personalized data while integrated with other security features to prevent harvesting. Embedded security features should also be very difficult to harvest by having unusual shapes.
- Diffractive optically variable image devices (DOVIDs) that are highly complex, technologically advanced, and not commercially available. DOVID designs must be easy to recognize (large surface areas, high optical brilliance), easy to remember (simple motif or logo), and easy to verify (by simple tilting or rotation of the card).

COUNTERFEIT DRIVER'S LICENSES: AN INCREASING THREAT

- Unique chemical characteristics that are part of the substrate, or ink chemical components, that can be detected using advanced forensic analytical equipment. These can be inherent or added as taggants.

Personalization technologies

- Laser engraving, which embeds personal information into the sub-surface layer(s) of the card body, eliminating the possibility of data alteration without tamper evidence.
- Special laser techniques allowing for personalization options such as micro printing, variable font size and images, and variable laser energy. This enables different print intensities to create (i) raised tactile printing above the plane of the card, (ii) engraved/debossed printing below the plane, and/or (iii) perforated designs.
- Laser engraved features (i) that use lenses such as Multiple or Changeable Laser Images or Floating Images, (ii) specific high-resolution fine line features, and (iii) high-resolution grey-scale images.
- Laser perforated photo in all layers of the card that uniquely matches the license to the person.
- Laser personalization that is integrated – via ablation – with other security features, such as DOVIDs and security features incorporated in complex windows.

FOR MORE INFORMATION:

info@documentsecurityalliance.org

515 2nd St NE | Washington, DC 20002
202-543-5552

DSA
ENHANCING DOCUMENT AND IDENTITY SECURITY

REFERENCES

1. https://www.cbp.gov/newsroom/local-media-release/over-19k-fraudulent-ids-seized-cbp-officers-chicago
2. https://www.javelinstrategy.com/content/2021-identity-fraud-report-shifting-angles-identity-fraud
3. https://www.justice.gov/usao-ri/pr/three-indicted-id-theft-fraudulent-credit-card-scheme
4. https://pubmed.ncbi.nlm.nih.gov/16736071/#:~:text=The%20estimated%20%2461.9%20billion%20bill,in%20lost%20quality%20of%20life
5. https://www.cnbc.com/2021/03/23/consumers-lost-56-billion-dollars-to-identity-fraud-last-year.html
6. https://www.sheerid.com/blog/how-many-fake-ids-are-in-your-returns-database/
7. https://www.stimson.org/wp-content/files/file-attachments/CT_Spending_Report_0.pdf
8. https://www.wsj.com/articles/rise-in-check-fraud-could-motivate-treasurers-to-switch-to-other-payment-tools-11579131505
9. https://www.aba.com/news-research/research-analysis/deposit-account-fraud-survey-report#
10. https://www.jsad.com/doi/abs/10.15288/jsa.2006.67.519
11. https://www.niaaa.nih.gov/publications/brochures-and-fact-sheets/underage-drinking
12. https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf
13. https://www.javelinstrategy.com/coverage-area/2020-identity-fraud-study-genesis-identity-fraud-crisis
14. https://www.sheerid.com/blog/how-many-fake-ids-are-in-your-returns-database/
15. https://www.stimson.org/wp-content/files/file-attachments/CT_Spending_Report_0.pdf
16. https://www.stimson.org/wp-content/files/file-attachments/CT_Spending_Report_0.pdf
17. https://www.documentsecurityalliance.org/ 3.7 million counterfeit driver licenses purchased annually multiplied by an average price of $130 = $481 million
18. https://www.cbp.gov/newsroom/local-media-release/over-19k-fraudulent-ids-seized-cbp-officers-chicago
19. https://educationdata.org/college-enrollment-statistics
20. https://www.thelantern.com/projects/2021/04/28/fake-ids-join-textbooks-and-shower-caddies-on-the-college-packing-list-find-popularity-regardless-of-legal-and-university-consequences/
21. http://pubs.sciepub.com/ajphr/5/6/3/index.html
22. https://www.pewresearch.org/fact-tank/2021/06/22/digital-divide-persists-even-as-americans-with-lower-incomes-make-gains-in-tech-adoption/
23. https://www.regulations.gov/document/DHS-2006-0030-10707
24. https://www.fbi.gov/news/stories/phony-document-rings-broken-up