HID

Unmasking the Threat:

Addressing Identity Document Fraud in Passports

Since the inception of the practice of using documents to identify individuals, there have been criminals who have attempted to create fraudulent identity documents, with various degrees of success. And since the origins of identification fraud, police, border and other relevant agencies have worked tirelessly to combat it. The financial, political and social impact of identification fraud is devastating and can have far-reaching consequences. Why? Simply put, fraudulent identity documents allow criminal enterprises to thrive.

This white paper will cover the scope and scale of identity document fraud, its impact on governments and citizens, the main areas of attack in passport fraud and, most importantly, strategies and solutions for combating passport fraud.

Geopolitical Pressure and Instability Driving Up Identity Fraud

The prevalence of fraudulent and counterfeited passports can be hard to track for the very simple reason that when it works, those numbers are not detected or reported. There are however indicators that provide an overview of the scale of the problem.

Natural distastes and geopolitical instability, marked by numerous conflicts worldwide has led to a surge in cross-border migration. Amid the individuals and families seeking refuge and safety from these crises, there is an increased risk of high-risk individuals entering undetected among the refugees.

Criminal networks often adjust their business model to the new reality, exploiting the increased migratory pressure on external borders and deteriorating socio-economic and humanitarian conditions.

According to the European Border and Coast Guard Agency Frontex, 2023 saw approximately 380,000 instances of unauthorized border crossings at the EU's external border, the "highest level since 2016, [constituting] a 17 percent increase from the figures in 2022, indicating a consistent upward trend over the past three years."

According to the Frontex 23/24 report:

- Document fraud continues to be a key enabler of threats at the EU's external borders. In 2022, the number of fraudulent documents reported within the European Union Document Fraud Risk Analysis Network (EDF-RAN) increased by 5% in relation to 2021. EU Member States/ Schengen Associated Countries in 2022 detected a total of 19,341 users of fraudulent documents (or in possession thereof) and 26,249 fraudulent documents at the EU's external borders and in intra-EU/ Schengen secondary movements.
- **Passports became the most reported fraudulent document type within ED-FRAN in 2022, with an increase of 35% relative to 2021**
- Counterfeit documents and impersonation were the most commonly reported types of fraud, accounting for 64% and 15% of detections of document related fraud in 2022 respectively

Learn more about how HID works with governments to create passports that are as secure as they are beautiful >>

HID

THE IMPACT OF PASSPORT FRAUD ON GOVERNMENTS

The fraudulent use of passports by criminals and terrorists can have severe implications for governments and their citizens, posing significant risks to national security, public safety and international relations. Some of the key implications include:

Terrorism and Illegal Activities: Fraudulent passports enable criminals and terrorists to travel across borders undetected, facilitating various illegal activities such as terrorists attacks, human trafficking, drug smuggling, arms trafficking and more.

Compromised Border Security: Illegal entry or exit through the use of fake passports undermines the integrity of border controls, making it harder for authorities to monitor and regulate the movement of individuals.

Identity Theft and Fraud: Fraudulent passports can be part of a larger scheme involving identity theft, enabling criminals to commit financial fraud, access sensitive information, or engage in other illicit activities using the stolen identity.

Damage to International Relations: Instances of passport fraud can strain diplomatic relations between countries, especially if it's found that the documents were forged or obtained through lax security measures in another country.

Undermining Trust in Travel Documents: Incidents of passport fraud can erode trust in official travel documents issued by governments. This could lead to stricter visa requirements, increased scrutiny for travelers, and additional bureaucratic procedures, impacting legitimate travelers.

Challenges for Law Enforcement: Detecting fraudulent passports requires experienced andtrained personnel. The existence of fake documents adds to the straining of valuable Government resources such as cost and time invested in continually train law enforcement personnelso as to identify and apprehend those using

Financial Costs: Addressing passport fraud involves significant financial costs for governments, including the training of personnel and upgrading technology for border security. There is also the economic impact tied to the loss of tax revenue from tax evasion and illicit financial transactions, the cost of investigating and prosecuting cases of identity document fraud and the cost of fraudulent claims to social services.

MAIN AREAS OF ATTACK IN PASSPORT FRAUD

Fraudulent passport activity takes many forms, involving both genuine documents and fake or altered documents:

Forged Document

Many forgeries start with alteration or replacement of the datapage one of the first viewed aspects of any Level One passport verification check. Datapge is the most attacked page as it contains all biometric and biographic data that is used for identification purposes.

Fraudulently Obtained Document

Presenting genuine certificates such as birth certificates to obtain authentic identification documents is also a major challenge for governments as it complicates the detection process. Since the verification process will not reveal the underlying fraud, the process to obtain document is vital in preventing such cases. This is why personal information on a datapage needs to be specifically protected. A recent security advancement (trend) is the multiplication of the portrait placed in different places across the passport through different technologies.

Counterfeited Document

As criminals gain access to technologically advanced components and technologies—such as lasers, manufacturing equipment, holographic origination systems, and face morphing techniques—issuing authorities must continuously advance and evolve their passport security features and protocols. Regular redesign of document security features are essential to stay ahead of counterfeiters and effectively protect national security.

STRATEGIES AND SOLUTIONS FOR COMBATING PASSPORT FRAUD

As a starting place, all passports should comply with the International Civil Aviation Organization's (ICAO) Doc 9303, which outlines a number of features that identity documents should contain, from machine readability to cryptographic protocols. However, successfully combatting the constantly evolving wave of identity document fraud involves the combination of multiple security features, technologies and personalization techniques that go beyond ICAO guidelines. This strategy ultimately raises the stakes to fraudster when it comes to releasing a credible counterfeited document.

Designing your countries' identity document is one of the most important things you will ever be involved in and as such it is imperative you understand the different elements involved. Firstly, there are three levels of security that are examined in different ways including sight/touch, magnifying glass/UV lamp and forensic authentication by professionals such as border guards."

Level 1 security features are a great start as they are easily detected and widely known among professionals. These can be in the form of changeable or multiple laser image where several portraits (usually 2) can be seen depending on the viewing angle. Level 2 take security to the next level by incorporating tiny elements into the base material of the document and these only emerge under UV lamp. Level 3 provides a high spec security that requires a specialist detector tool.

If you are seeking a highly secure document, combining various technologies and methodologies to protect different parts of the document with distinct features is the best approach.

While the ICAO recommends redesigning every 10 years, fraudsters can catch up and master these technologies within that time-frame, finding new ways to breach the system. Therefore, redesigning your country's identity document every 5-10 years would be a sensible strategy to maintain a high level of national security while maintaining international standards to ensure compliance and global interoperability.

OUR RECOMMENDATION;

- HID Mirage™ — a unique window feature combining negative laser personalization, a bi-color metallic effect, watermark effect, vanishing image and window seal.

- HID® Safelink — a feature designed to protect the hinge (attaching the data page to the rest of the passport), which includes a UV print pattern to prevent against any attempted data page alteration or replacement

BUILDING A SECURE FUTURE FOR PASSPORT AUTHENTICATION

Reducing identity document fraud in passports will continue to be of paramount importance for the foreseeable future. The dangers posed to governments and citizens from fraudulent documents — from the diminished credibility of their identity verification systems to the very tangible and wide-reaching economic and social risks — will continue as long as there are criminals willing to exploit passport vulnerabilities for profit. To successfully stay ahead of criminal advancements in counterfeiting and fraud technology, governments and industry experts must take a comprehensive, collaborative and pro-active approach.

Explore the features of a modern, secure passport >>