Diverse Authentication Library

# Deep Fakes

## The Surge of AI-Generated Synthetic Identities and Unveiling the Amplified Threats

By Dawid Jacobs and Debbie Reynolds

## Introduction

The rapid proliferation of synthetic identities, accompanied by a worrying increase in associated criminal activities, has become an urgent issue demanding immediate attention. These concerning trends beg the question: Why, despite the abundance of Identity Verification Solutions, does this problem persist?

While the answer may appear straightforward, it masks a complex web of challenges that make resolving this issue a daunting task.

## The Inadequacies of Existing Identity Verification Solutions

Identity verification methods that rely on "selfie-based authentication," "liveness detection," and even advanced "Artificial Intelligence" (AI) algorithms, are falling behind in the race against ever-evolving criminal syndicates. These criminal groups have mastered the art of producing intricate Deep Fakes, skilfully manipulating these technologies to expose and exploit their inherent vulnerabilities. Their expertise in creating sophisticated Deep Fakes has enabled them to exploit vulnerabilities within these Identity Verification Solutions, consistently refining their techniques to generate a rapidly growing number of Synthetic Identities.

## Related articles:

- Will Deepfakes Kill Identity Verification?
  blogs.gartner.com/akif-khan/will-deepfakes-kill-Identity-verification/

- Note that two phones are at work when defrauding the victim. The first phone applies a filter to disguise the criminal's face, presenting it as someone else entirely. Meanwhile, the second phone is directed at the first one, revealing the altered face of the criminal. Post | Feed | LinkedIn

- Martin Lewis has warned people not to fall victim to a scam artificial intelligence (AI) generated video that appears to show him endorsing a fake investment project from Elon Musk.
  'Absolutely terrifying': Martin Lewis issues warning after deep fake video of him appears online | ITV News

- Identity checks on crypto exchanges at risk as AI deepfakes evolve –
  Identity checks on crypto exchanges at risk as AI deepfakes evolve (cointelegraph.com)

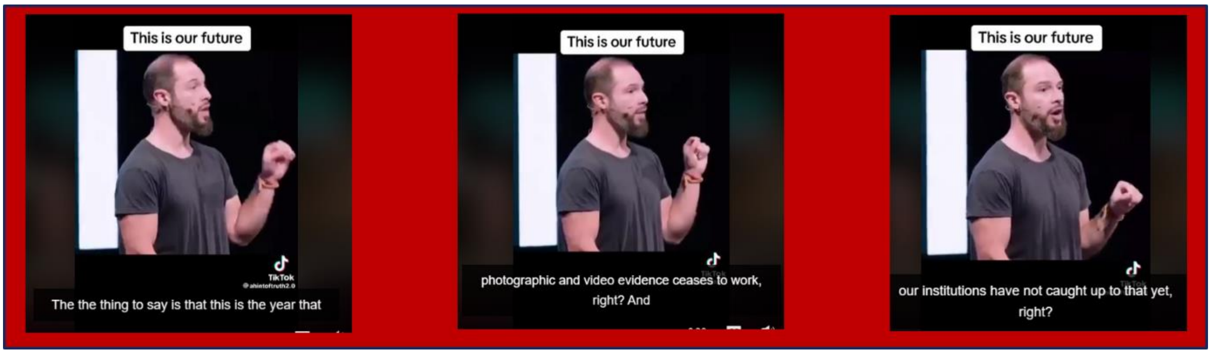
- Synthetic Identity Is Back With A Vengeance – Frank on Fraud
  (In this instance, the Synthetic Identities are not back. They have matured over the last couple of years and are now starting their path of destruction – Dawid Jacobs)

- Post | Feed | LinkedIn
  (The sheer fact that Smile ID (formerly Smile Identity) gave me (Caleb MaruCaleb Maru) their data on 75 million identity checks across Africa, should undoubtedly evoke profound apprehension within every individual.)

This Deep Fake, document is the exclusive creation and property of Dawid Jacobs. Any form of copying or distribution of this document is strictly prohibited unless expressly authorized in writing by Dawid Jacobs.

## Alarmingly, many of the existing Identity Verification Solutions are predicted to become obsolete in as little as one year

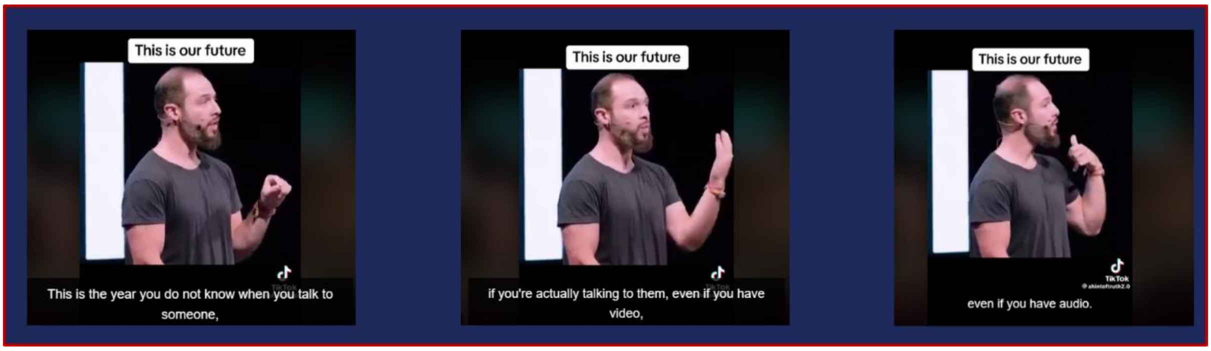
- Replying to @Time VS Journey Artificial Intelligence will be able to e... | Artificial Intelligence | TikTok *(In the TikTok video, the commentator suggests that the quality of fabricated photos, videos, and voices of individuals will reach a point where discerning whether you're interacting with an actual human being will become increasingly challenging, even impossible - Dawid Jacobs)*



The the thing to say is that this is the year that

photographic and video evidence ceases to work, right? And

our institutions have not caught up to that yet, right?



This is the year you do not know when you talk to someone,

if you're actually talking to them, even if you have video,

even if you have audio.

Furthermore, the issue amplifies when even a single Synthetic Identity infiltrates any system, opening the door to considerable data, financial, and reputational losses. While present Identity Verification Solutions may prove lucrative for providers, viewing Synthetic Identity as solely a data problem that can be resolved through digital comparisons disregards the fundamental issue—Synthetic Identities are intrinsically rooted in human manipulation. The problem escalates when unprepared buyers invest in solutions that fail to address the underlying challenges, thereby exacerbating the imminent challenges of the situation.

## The Flaw in Current Approaches to Identity Verification Solutions

The Management of Human Identity and Identity Verification Solutions transcend mere data collection and require profound respect for individual uniqueness. An individual's Identity isn't simply a compilation of data points; it's a substantive testament to their real-world existence. Effective Identity Management incorporates the core tenets of Records Management, seamlessly integrating them into every aspect of human Identity.

This Deep Fake, document is the exclusive creation and property of Dawid Jacobs. Any form of copying or distribution of this document is strictly prohibited unless expressly authorized in writing by Dawid Jacobs.
dal-identity.com I dawid@dal-identity.com

To effectively combat the rise of Synthetic Identities, it is essential to adopt a more focused approach to Identity Management, coupled with a cessation of undervaluing the uniqueness of the individual. Recognizing Human Identity as a definitive record of their physical presence underscores the critical importance of ensuring unquestionable certainty in engaging with real-world individuals, preventing Synthetic Identity infiltration.

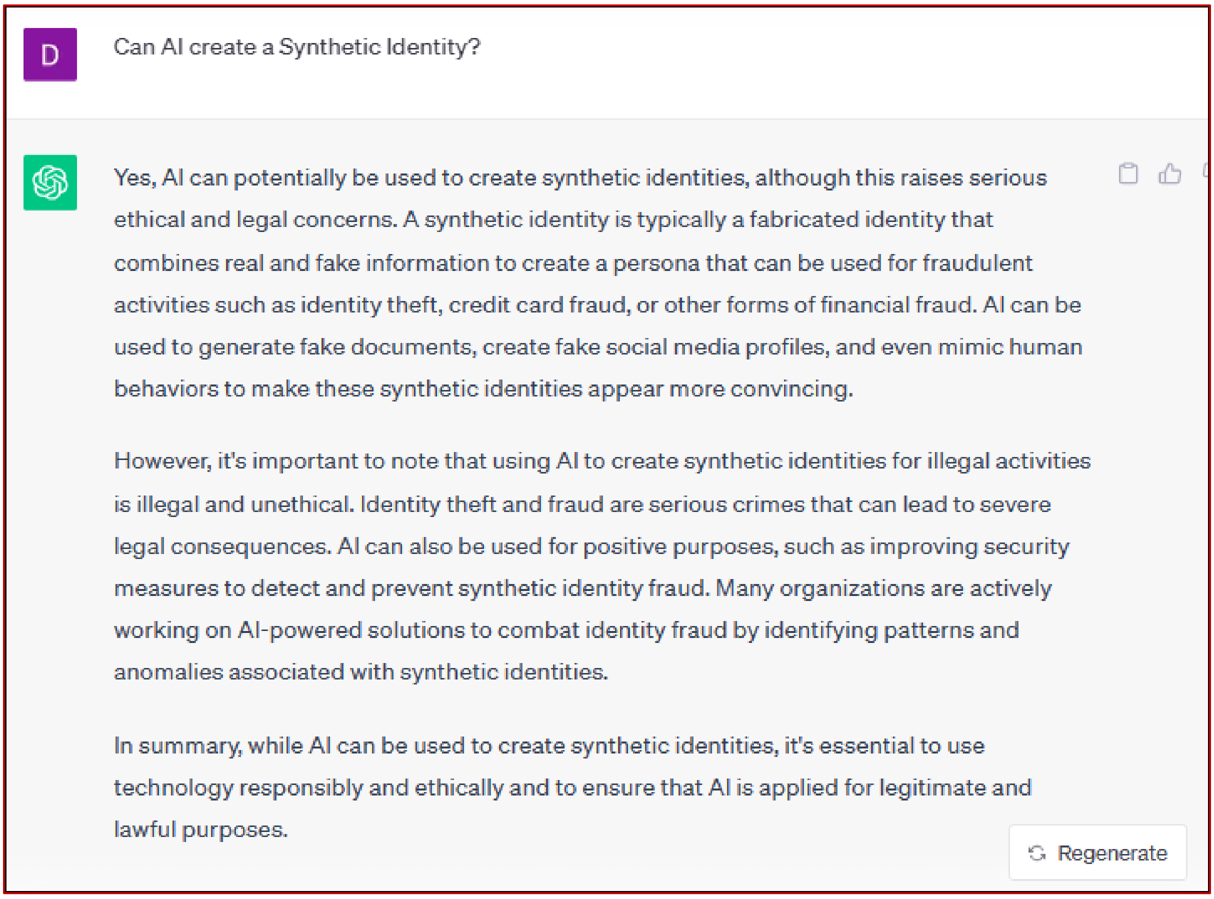
## The Escalating Threat of AI-Generated Content and Identity Verification Solutions

The exponential rise of AI-generated content has unleashed a host of formidable challenges, warranting heightened vigilance and preparedness, in the realms of Synthetic Identities and Deep Fakes.

The unchecked growth of AI-generated content directly corresponds to the amplified risk of AI-crafted Synthetic Identities and Deep Fakes – a hazard that transcends boundaries, affecting individuals, institutions, and governments alike. The impending scale of this predicament is undeniable, with current Identity Verification Solutions ill-equipped to counteract the infiltration of Synthetic Identities into various systems.

The Synthetic Identities stemming from AI-generated entities serve a diverse range of illicit activities, from compromising financial systems to manipulating political outcomes. This emergence presents numerous concerns that necessitate an immediate and comprehensive examination of its multifaceted impacts.

Asking AI directly if AI-generated Synthetic Identities is possible……..



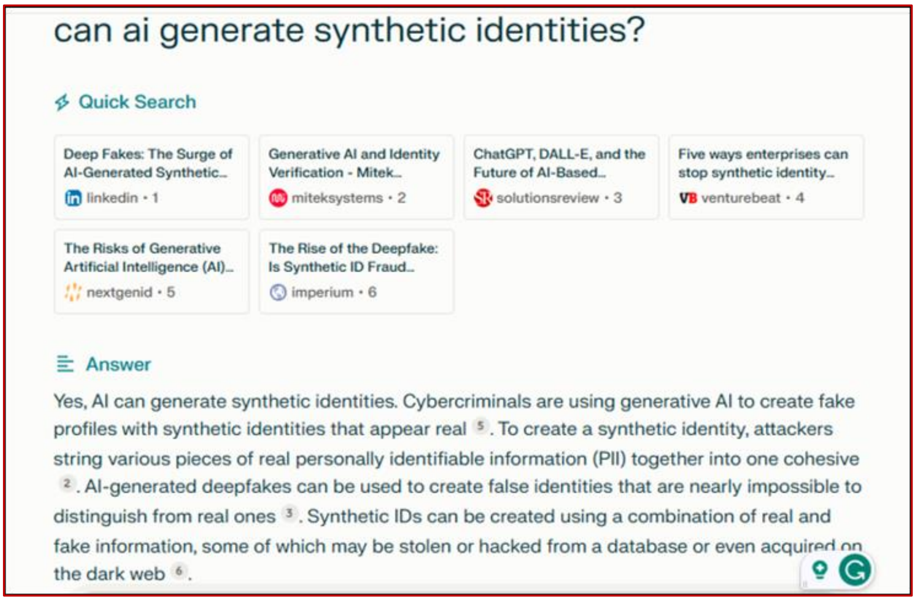
Can AI create a Synthetic Identity?

Yes, AI can potentially be used to create synthetic identities, although this raises serious ethical and legal concerns. A synthetic identity is typically a fabricated identity that combines real and fake information to create a persona that can be used for fraudulent activities such as identity theft, credit card fraud, or other forms of financial fraud. AI can be used to generate fake documents, create fake social media profiles, and even mimic human behaviors to make these synthetic identities appear more convincing.

However, it's important to note that using AI to create synthetic identities for illegal activities is illegal and unethical. Identity theft and fraud are serious crimes that can lead to severe legal consequences. AI can also be used for positive purposes, such as improving security measures to detect and prevent synthetic identity fraud. Many organizations are actively working on AI-powered solutions to combat identity fraud by identifying patterns and anomalies associated with synthetic identities.

In summary, while AI can be used to create synthetic identities, it's essential to use technology responsibly and ethically and to ensure that AI is applied for legitimate and lawful purposes.

This Deep Fake, document is the exclusive creation and property of Dawid Jacobs. Any form of copying or distribution of this document is strictly prohibited unless expressly authorized in writing by Dawid Jacobs.
dal-identity.com I dawid@dal-identity.com



can ai generate synthetic identities?

Deep Fakes: The Surge of AI-Generated Synthetic… linkedin • 1

Generative AI and Identity Verification - Mitek… miteksystems • 2

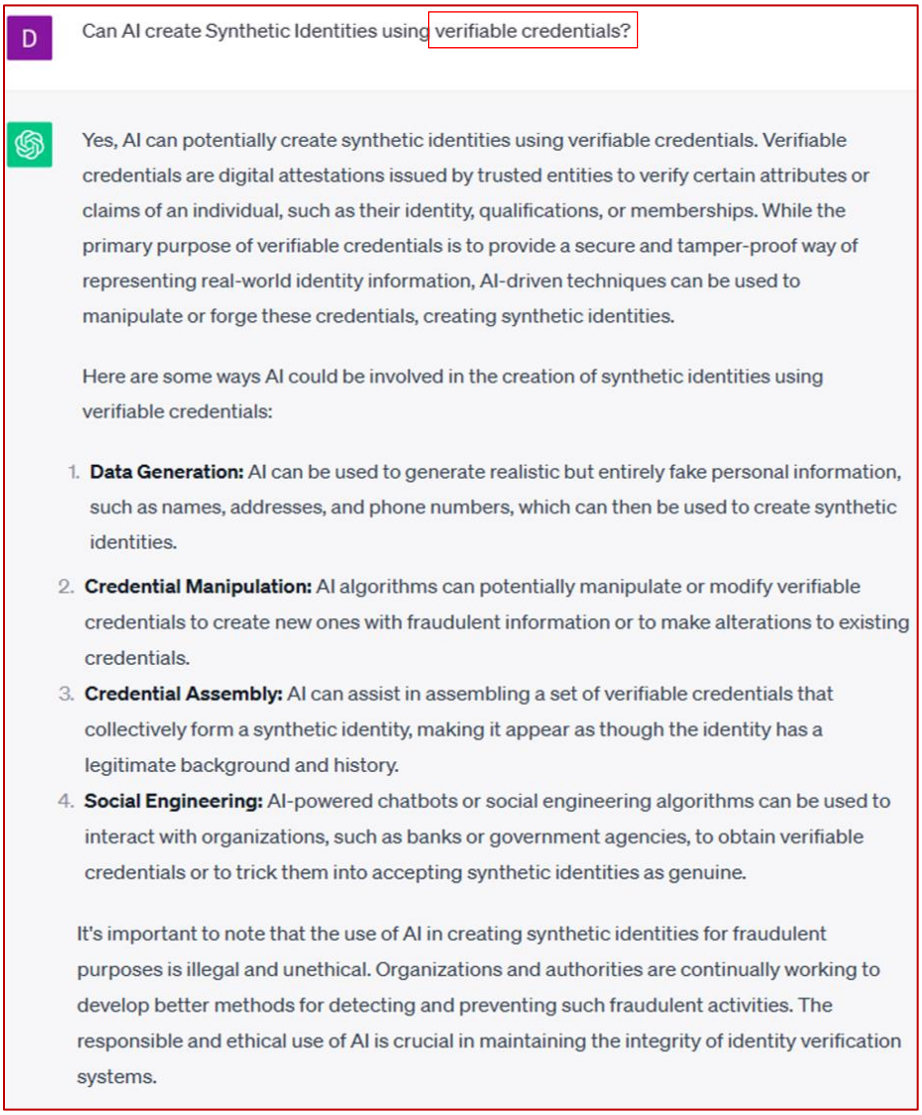
ChatGPT, DALL-E, and the Future of AI-Based… solutionsreview • 3

Five ways enterprises can stop synthetic identity… venturebeat • 4

The Risks of Generative Artificial Intelligence (AI)… nextgenid • 5

The Rise of the Deepfake: Is Synthetic ID Fraud… imperium • 6

Yes, AI can generate synthetic identities. Cybercriminals are using generative AI to create fake profiles with synthetic identities that appear real [5]. To create a synthetic identity, attackers string various pieces of real personally identifiable information (PII) together into one cohesive [2]. AI-generated deepfakes can be used to create false identities that are nearly impossible to distinguish from real ones [3]. Synthetic IDs can be created using a combination of real and fake information, some of which may be stolen or hacked from a database or even acquired on the dark web [6].



Can AI create Synthetic Identities using verifiable credentials?

Yes, AI can potentially create synthetic identities using verifiable credentials. Verifiable credentials are digital attestations issued by trusted entities to verify certain attributes or claims of an individual, such as their identity, qualifications, or memberships. While the primary purpose of verifiable credentials is to provide a secure and tamper-proof way of representing real-world identity information, AI-driven techniques can be used to manipulate or forge these credentials, creating synthetic identities.

Here are some ways AI could be involved in the creation of synthetic identities using verifiable credentials:

1. **Data Generation:** AI can be used to generate realistic but entirely fake personal information, such as names, addresses, and phone numbers, which can then be used to create synthetic identities.
2. **Credential Manipulation:** AI algorithms can potentially manipulate or modify verifiable credentials to create new ones with fraudulent information or to make alterations to existing credentials.
3. **Credential Assembly:** AI can assist in assembling a set of verifiable credentials that collectively form a synthetic identity, making it appear as though the identity has a legitimate background and history.
4. **Social Engineering:** AI-powered chatbots or social engineering algorithms can be used to interact with organizations, such as banks or government agencies, to obtain verifiable credentials or to trick them into accepting synthetic identities as genuine.

It's important to note that the use of AI in creating synthetic identities for fraudulent purposes is illegal and unethical. Organizations and authorities are continually working to develop better methods for detecting and preventing such fraudulent activities. The responsible and ethical use of AI is crucial in maintaining the integrity of identity verification systems.

Verifiable Credentials **will** be used in AI-generated Synthetic Identities

## Key Concerns and Urgent Examination regarding Deep Fakes and Identity Verification Solutions

1. **Magnitude and Velocity**: AI algorithms are poised to produce Synthetic Identities at an unprecedented rate, overwhelming traditional Identity validation systems, including "selfie solutions" and purported "AI" alternatives. Given the potential for the global population to rapidly multiply, distinguishing between real individuals and Synthetics will become an exceedingly challenging endeavor.

2. **Sophistication**: AI-generated Synthetic Identities flawlessly mimic human traits, compounding the risk of fraud and malicious activities.

3. **Detection Evasion**: As AI advances, the Synthetic Identities it generates become adept at exploiting existing and future security vulnerabilities, masquerading as legitimate users. Even mechanisms labeled as "AI Identity-based" will likely fall short in recognizing AI-generated Synthetic Identities.

4. **Multifaceted Mimicry**: AI-generated Synthetic Identities encompassing biometric markers, especially facial recognition and voice biometrics and personal data evade easy detection, even profiting from Identity Verification Solutions.

5. **Magnified Data Breaches**: Synthetic Identities amplify data breach risks and consequences, amplifying data losses, inflating financial losses, and increasing reputational damage.

6. **Trust Erosion**: Pervasive AI-generated Synthetic Identities corrode trust in digital platforms, hampering user confidence and business functionality.

7. **Money Laundering and Fraud**: AI-forged Synthetic Identities provide a cloak for illicit transactions and activities.

8. **Regulatory Complexities**: Regulators face significant challenges in enforcing Identity validation and compliance standards against AI-generated Synthetic Identities.

9. **Disruption of Trust Systems**: Synthetic Identities disrupt core trust systems, eroding reputation mechanisms and online reviews.

10. **Cybercrime:** The emergence and proliferation of synthetic identities have introduced a significant and complex threat landscape within the realm of cybercrime. This form of cybercrime has far-reaching implications and has become a critical concern for individuals, businesses, and governments alike. The scale of synthetic identity fraud is enormous. Determining accountability and implementing effective regulations to combat this type of cybercrime can be complex due to the intricate and global nature of these schemes.

    - *"Cybersecurity Ventures expects global cybercrime costs to grow by 15 percent per year over the next three years, reaching $8 trillion USD globally this year and $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015."* 2023 Cybersecurity Almanac: 100 Facts, Figures, Predictions, And Statistics (cybersecurityventures.com)

This Deep Fake, document is the exclusive creation and property of Dawid Jacobs. Any form of copying or distribution of this document is strictly prohibited unless expressly authorized in writing by Dawid Jacobs.

The impact of synthetic identities on cybercrime is substantial and multifaceted. The dynamic and adaptive nature of these identities challenges traditional security measures and requires a collaborative and proactive approach to mitigate their effects on individuals, businesses, and the broader digital ecosystem.

## DAL Identity: The Proactive Solution against Synthetic Identities: Embracing Genuine Identity Management

The surge in Synthetic Identities and their associated threats has reached alarming levels, necessitating a robust and comprehensive solution to counter this evolving menace. In response to this pressing challenge, DAL Identity emerges as a groundbreaking solution aimed at neutralizing the proliferation of Synthetic Identities, whether devised by criminal syndicates or facilitated by the advancing realm of AI-generated counterparts. This innovative approach is rooted in the profound recognition that an individual's Identity is a tangible manifestation of their presence in the real world. By steadfastly upholding this principle, DAL Identity not only acknowledges the intrinsic significance of Identity but takes actionable steps to safeguard it against manipulation.

## The Essence of True Identity Management

Genuine Identity Management encompasses a deep reverence for the uniqueness of each individual. An individual's Identity stands as irrefutable evidence of their distinct existence in the tangible realm. To this end, effective Identity Management must encompass the core principles outlined in Records Management, seamlessly applied across every dimension of human Identity. DAL Identity operates on the premise that Identity is not merely a data point, but a testament to a genuine person's presence in the physical world.

## Countering Synthetic Identities: A Holistic Approach

The proactive solution to thwart Synthetic Identities necessitates a multifaceted strategy that embraces the individual as the focal point of Identity Management. Recognizing the intrinsic value of Human Identity as a tangible representation of one's presence underscores the critical need for unwavering certainty in interactions with real-world individuals, thereby thwarting the infiltration of Synthetic Identities.

To effectively counter this escalating threat, the following strategic elements must be employed:

1. **Multi-Modal Biometrics with Forensic Protocol**: Employing multi-modal biometrics fortified by forensic protocols, encompassing fingerprints, DNA, iris scans, and facial images, enhances Identity verification precision. This step is vital in foiling attempts by AI-generated Synthetic Identities to breach security.

2. **Forensic Cryptography Provenance**: The integration of end-to-end encryption, tokenization, and robust key management guarantees data integrity, confidentiality, and accessibility. This fortifies digital security and plays a crucial role in identifying cybercriminals and pre-empting imminent attacks.

3. **Enhanced KYC and AML Procedures**: Strengthening Know Your Customer (KYC) and Anti-Money Laundering (AML) protocols ensures that identities linked exclusively

to real-world individuals are embraced. This step effectively prevents the creation of synthetic identities and curbs their subsequent malicious activities.

4. **Regulation and Compliance**: Governments and regulatory bodies assume pivotal roles in enforcing stringent regulations that stipulate forensic Identity verification standards. Such measures mitigate data privacy risks and thwart large-scale Synthetic Identity incursions.

## Conclusion

Though the specter of AI-generated Synthetic Identities casts an ominous shadow, it also begets opportunities for innovation and resilience. Leveraging advanced forensic-based Identity Management solutions intertwined with regulatory frameworks, collaborative efforts, and preemptive security measures empowers institutions to thwart Synthetic Identity risks, now and into the future.

The collective response of institutions, governments, forensic experts, and technology professionals is pivotal in safeguarding all sectors' integrity amidst this evolving threat. By adeptly navigating emerging challenges and leveraging innovative solutions, any sector can chart its course while upholding trust, security, and stability. Employing advanced forensic-based Identity Management solutions with forensic cryptographic provenance technology-driven solutions, alongside regulatory frameworks, collaborative efforts, and proactive security measures, empowers institutions to identify and nullify risks from Synthetic Identities.