`

STATE BAR OF WISCONSIN
PINNACLE
Your Practice. Our Purpose.

WSSFC 2025

Plenary 3

Navigating Deepfake Technology

Presenters:
Cheryl (Cheri) A. Hipenbecker, Knight Barry Title, Inc., Milwaukee
Prof. Derek Riley, Ph.D., Milwaukee School of Engineering, Milwaukee

About the Presenters...

Cheryl (Cheri) A. Hipenbecker is General Counsel with the Knight Barry Title Group. She received her undergraduate degree from the Winona State University in Political Science, and her law degree from University of Minnesota magna cum laude. After graduation, Cheri worked with the law firm of Hostak, Henzl & Bichler in Racine before joining Knight Barry Title in 2007. Cheri is a past president of the Wisconsin Land Title Association (WLTA), current Legislative Chair of the WLTA and current member of the Town of Norway Planning Commission & Land Use Committee.

Derek Riley, Ph.D., is a professor and the director of MSOE's Computer Science program, which includes an emphasis in artificial intelligence and deep learning. His teaching and research areas include machine learning, modeling, and high performance computing. Derek got his PhD at Vanderbilt University in 2009 where he developed high performance formal modeling and simulation methods for biochemical and industrial systems. In addition to teaching at MSOE, he provides data, algorithm, LLM, and AI consulting services, and is a member of the Association for Computing Machinery.

October 17th, 2025

Knight Barry TITLE GROUP

MSOE UNIVERSITY

NAVIGATING DEEPFAKE TECHNOLOGY

(the Criminals Are Winning)

PRESENTED BY

Cheri Hipenbecker
General Counsel | Knight Barry Title

Dr. Derek Riley
Professor, Program Director | MSOE

1

$1M vacant land sold Feb. 2024 -

Seller Impersonation Fraud with Synthetic IDs

- Couple left distraught after peaceful $1 m plot of land where they planned to retire was stolen from them
- American Land Title Association – Seller Impersonation Fraud

2

Confirming Remote Identities

- Request multiple forms of identity verification
- Check images and documents thoroughly
  - Reference image, signatures
- Talk to the person
  - Use a reference voice
- Conduct video calls to confirm real-time presence
- Control the Signing!!!

3

ID Verification– Due Diligence

- Suppose you can find a video of someone being interviewed
  - Image
  - Audio
  - Video
- Images
  - Ask for a photo of the person signing a document, check it!
- Audio
  - Talk to them on the phone, see if they sound similar!
- Video
  - Set up a video call to see if they look similar!

Wait, if you can find reference content online, so can imposters!

4

Example

YouTube clip posted publicly

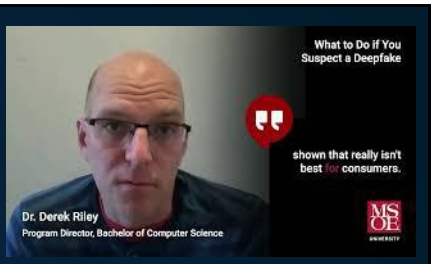
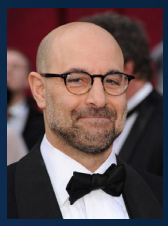
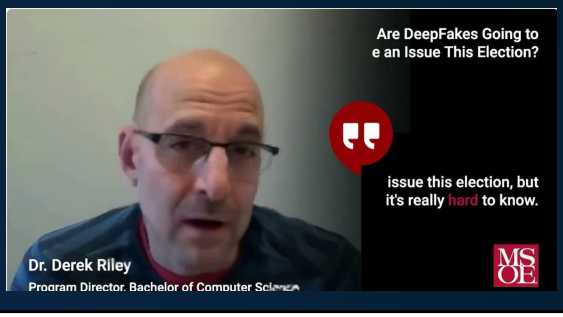


Image generated from screenshot using Google Gemini

Audio generated using resemble.ai



Video generated using remaker.ai



5

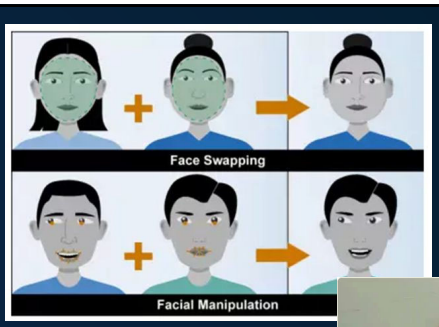
This is not Morgan Freeman (2021)

Knight Barry Title Group | MSOE University

6

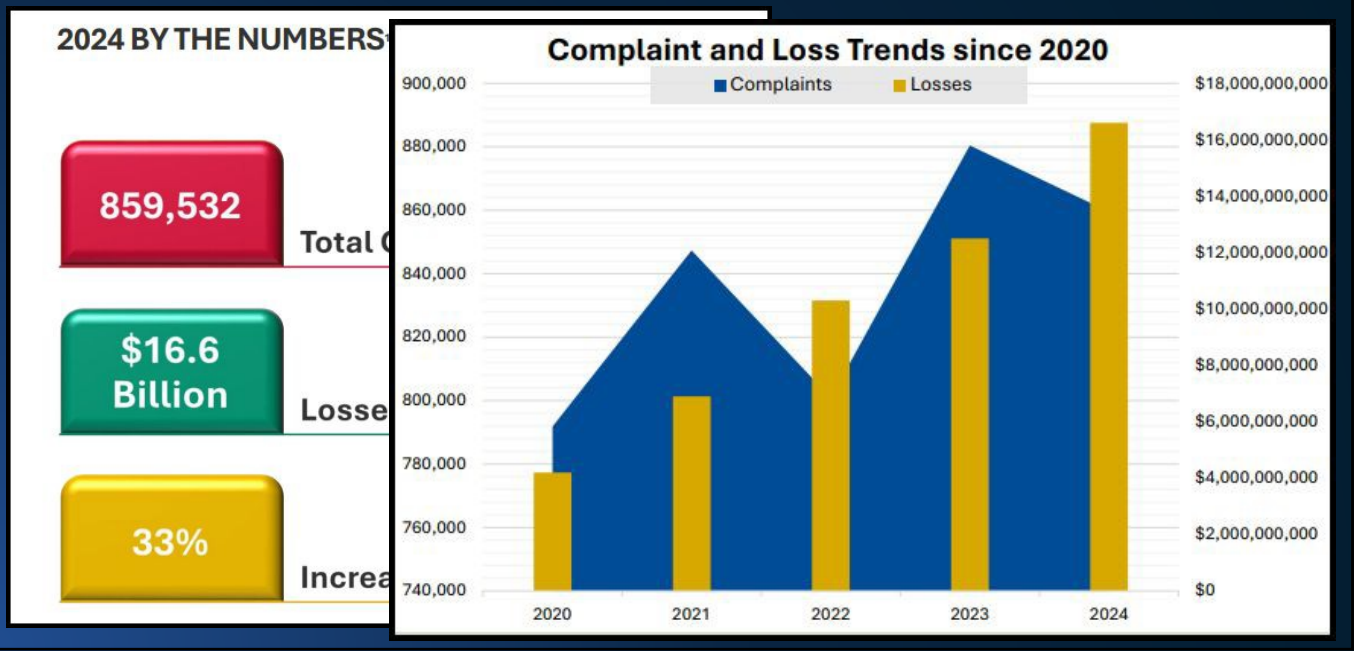
How does this work?

- Face Swapping
  - Faster, cheaper, easier, less fidelity
- Facial Manipulation
  - More complex, but higher quality
- How good are you at detecting what is real?
  - https://detectfakes.kellogg.nor
- Detecting Face Swapping
  - Ask the person to turn their head (liveness testing)



7

By the Numbers – FBI IC3 Annual Reports –www.ic3.gov



8

Where oh where do these losses come from?

BY COMPLAINT LOSS

Crime Type	Loss	Crime Type	Loss
Investment	$6,570,639,864	Extortion	$143,185,736
Business Email Compromise	$2,770,151,146	Lottery/Sweepstakes/ Inheritance	$102,212,250
Tech Support	$1,464,755,976	Advanced Fee	$102,074,512
Personal Data Breach	$1,453,296,303	Phishing/Spoofing	$70,013,036
Non-Payment/Non-Delivery	$785,436,888	SIM Swap	$25,983,946
Confidence/Romance	$672,009,052	Overpayment	$21,452,521
Government Impersonation	$405,624,084	Ransomware *	$12,473,156
Data Breach	$364,855,818	Harassment/Stalking	$10,611,223
Other	$280,278,325	Botnet	$8,860,202
Employment	$264,223,271	IPR/Copyright and Counterfeit	$8,715,512
Credit Card/Check Fraud	$199,889,841	Threats of Violence	$1,842,186
Identity Theft	$174,354,745	Malware	$1,365,945
Real Estate	$173,586,820	Crimes Against Children	$519,424
*Descriptor***			
Cryptocurrency	$9,322,335,911		

9

And so do the cybercriminals

2024 numbers from FBI

- 9,619 complaints
- 1,785 complaints from individuals 60+ (with $50,525,457 losses)
- $67,513,795 losses from cryptocurrency
- $169,942,495 total losses (ranked 23rd)

10

The Real Estate Sector (CertifID's 2025 State of Wire Fraud)

11

How are the CyberCriminals Winning?

They have your data and have access to your emails (unless secured)**

2024

- 2.8 billion passwords leaked or sold online
- 61% of breaches involved email addresses
- 39% included phone numbers
- 22% involved government–issued IDs

Verizon's 2025 Data Breach Investigations Report

12

How are the CyberCriminals Winning?

They can bypass your SMS Multi-Factor Authentication (MFA)

SIM-Swapping

- Fraudster convinces a mobile carrier to transfer the victim's number to a SIM card they control
- Fraudster now has control over calls, texts AND *one-time passcodes*
- SMS is insecure and unreliable
  - *Preview to a Solution: Time-based One-Time Passwords (TOTP) apps*

13

How are the CyberCriminals Winning?

They create ID's out of thin air

Synthetic IDs

- ID documents containing a mix of real and fake information
  - Legitimate ID number with a fake name or image
- Synthetic images can be created to match a photo on a forged document
  - Enabling the manipulation of facial recognition and KYC systems
- Synthetic identities are easy to make and can be very convincing

14

How are the CyberCriminals Winning?

They can get it *cheap*

- FraudGPT – $105/month. AI tool to create malware, build phishing pages, create scam letters…
- WormGPT – $110/month. Darker sibling to ChatGPT, AI tool to generate phishing messages, execute BEC attacks, and create malicious code.
- PassGAN – Open sourced AI-powered password-cracking tool. In a recent study, PassGAN cracked 51% of passwords in under a minute, 65% within an hour, and over 80% within a month

15

In the "Real" World

16

$19M lost July 2025 -

Business Email Compromise and Spoofed Email

- $19M Gone: Hackers Scam NYC Real Estate Giant with One Email, Homeland Security Now Investigating.
- Milford Firm Loses $19M in Phishing Scam, Faces Negligence Lawsuit
- NYC firm handling lux properties allegedly scammed out of $19M — thanks to single phishing email

17

$25M lost Feb. 2024 -

Deepfake Technology

- Finance Employee Defrauded for $25M by Deepfake CFO
- Arup lost $25Mn in Hong Kong deepfake video conference scam
- Inside the $25M Hong Kong Deepfake Scam: A Comprehensive Analysis

18

$1M vacant land sold Feb. 2024 -

Seller Impersonation Fraud with Synthetic IDs

- Couple left distraught after peaceful $1m plot of land where they planned to retire was stolen from them
- American Land Title Association – Seller Impersonation Fraud

19

Beyond Real Estate

- Ferrari executives were targeted with a deepfake scam
  - Phone messages and calls sounded like they came from the CEO
  - The originated from an unknown number
- One executive asked the caller about a recent book recommendation
  - That was enough to identify the call as a scam

As reported by Bloomberg, one of the messages read: "Hey, did you hear about the big acquisition we're planning? I could need your help." The scammer continued, "Be ready to sign the Non-Disclosure Agreement our lawyer will send you ASAP." The message concluded with a sense of urgency: "Italy's market regulator and Milan stock exchange have already been informed. Maintain utmost discretion."

20

Scenario-

You get a request to execute a transaction with a remote party

What should you request to confirm they are who they say they are?

21

Confirming Identity

Types

- Name
- Address
- Email
- Drivers License
- Voice (phone)
- Online meeting

Attacks

- Google
- Google
- Create a new one
- Photoshop/Deep Fake
- Deep Fake
- Deep Fake

22

What is the state of the art?

- Real-time video requires significant resources
  - Getting cheaper/easier, but still significant
- Video manipulation is mainstream in media
- 2024 Film “Here”

https://metaphysic.ai/tech-and-research/

23

Stopping the Madness

- **Building Trust**

24

Pause before you trust. If something feels off—STOP.

- Why is this so urgent?
- Verify through known phone # or an independent internet search for the phone number. Never rely on incoming call (b/c of real time voice cloning)
- Require 2 people for all payment changes
- Internal Code words (protect against the $25M Deepfake)

Everyone -

Stop and smell the roses. Zero $$ can save thousands.

25

Purpose: Verify identities to prevent fraud.

Questions: Is the Gov't ID authentic? Is the person presenting the ID the actual person on the ID?

Control the signing: don't simply let a signer select their own notary (prevent seller impersonation fraud)

Consider using technology:

Companies -

Create an Identity Fraud Prevention Program

**this is the new industry standard in the real estate title and settlement world – ALTA Best Practic

26

- Periodic training on fraud in all shapes and sizes
- Phishing simulations
- Measure staff performance
- Talk about fraud attempts and successes

Teams -

Instill a culture of security with a Security Awareness Program

27

- **Protect your data.**
  - Strong passwords.
  - Multi-Factor Authentication (authenticator app vs. SMS?)
  - Change eSIM card in cell phones (AT&T default =1111)
  - Freeze credit: Experian, Transunion and Equifax
  - Get an Identity Protection PIN from the IRS
- **Monitor and report.** Check your accounts and credit activity regularly.

Family -

Taking it home to your spouse and children.

28

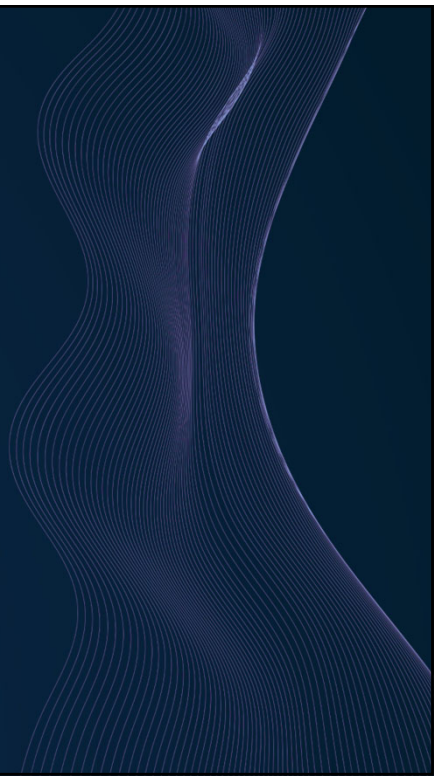
- More secure – Verified by the provider
- Examples: Google Authenticator and Microsoft Authenticator
- TOTP can be Phished, so they are not foolproof
- More security is possible
  - More factors– hardware keys, biometrics, digital certificates, etc.
  - BUT More security =morebarriers

Authenticator App

aka Time-Based One-Time Passwords (TOTP)

29

Steps if $$ lostvia wire fraud



30

Prepare NOW with a Wire Fraud Recovery Plan

- Who are your teams of people?
- Who will they call?
  - Sending bank – initiate wire recall
  - Recipient bank
  - Local Authorities
  - FBI (inc. report to ic3.gov)
  - Recovery services – https://www.certifid.com/solutions/recoveries
- Do you have the right insurance?

31

AI is scary - but at least now babies can work

32

Questions?
Reach Out

Cheri Hipenbecker
General Counsel
Knight Barry Title
cah@knightbarry.com

Dr. Derek Riley
Professor, Program Director | MSOE
riley@msoe.edu

33

ALTA BEST PRACTICES GUIDANCE - IDENTITY VERIFICATION

VERSION: 01.00
PUBLISHED 08-19-2025

ALTA Best Practices Executive Committee and Work Group

Contents

Summary – Purpose of this Guidance

Fraud and forgery concerns continue to be a growing and persistent challenge in processing financial and property transactions in all industries. Implementing identify verification processes, though presenting challenges such as potential transaction delays and privacy concerns, can provide significant benefits that far outweigh the risks to all parties in the real estate transaction, including:

- Robust identity verification effectively reduces seller impersonation fraud, safeguarding buyers from substantial financial losses and emotional distress.
- Builds trust in real estate platforms and agencies, fostering a healthier market environment.
- Provides crucial legal protection for all parties involved, creating a clear audit trail for potential disputes.
- Ensures compliance with increasingly strict regulations aimed at combating money laundering and fraud in real estate transactions.

ALTA Best Practices has continued to implement and update the requirements to address risks and threats to the real estate industry. In support of these changes, ALTA is providing this document to support the understanding and analysis of the available approaches to identity verification. Because the threats that identity verification are designed to prevent are emerging and evolving threats, this Guidance will be updated periodically as new threats emerge and as tools and approaches to combat these threats are improved. ALTA understands that no approach will prevent all fraud, but that effort appropriate to the risk should be made to mitigate fraud.

This Guidance is aimed at providing methods for a settlement agent to answer the following basic questions when presented with a government ID by a person who has signed or proposes to sign a conveyance document:

- Is this a valid government ID?
- Does the person on the government ID match the individual who presented it?
- Is the person on the government ID the actual seller, buyer, or borrower (as applicable) in the transaction?

This Guideline outlines some of the approaches that can be utilized but does not set a minimum standard or requirement for what methods to utilize. Some of the methods discussed may not be readily available to settlement agents. Thus, settlement agents may wish to consider engaging a technology company that may provide an option to utilize such tools.

Identity Verification Methods

The following section discusses the various methods of identity verification that are available. No method or methods completely eliminate the risk of impersonation or forgery, but the objective is to use the tools available to reduce the risk.

1. Verification of Government ID provided by a signer

- Description: Physical document verification of a government issued photo ID (driver's licenses, passports). Designed to answer the question: Does the individual possess an authentic Government issued identity document that supports their claim to a physical identity?
- Potential actions to verify:
  - Where possible, obtain and validate the ID of a signer in advance of the closing.
  - Require multiple forms of government ID, at least one of which is unexpired.
  - Cross referencing data sources: Data in the government ID cross-referenced with DMV database, or similar, to determine if:
    - ✓ The database corroborates the ID and the provided personal information
    - ✓ The expiration date, issue date, and id number can be verified
    - ✓ The data in the ID cross-references with data provided using the bar code or other similar coding.
  - Tamper and manipulation detection methods (color, text patterns).
  - Automated security feature detection (holograms, UV patterns).
  - The expected features of the government ID of the jurisdiction.
  - Use of systems or tools to identify forged government IDs:
    - ✓ Print quality and color matching: Advanced systems check for inconsistencies in print quality and color across the document, which may indicate physical alterations.
    - ✓ Font consistency analysis: Systems examine the consistency of fonts used throughout the document to identify potential tampering.
    - ✓ Photo replacement detection: Some fraudsters physically replace the photograph on a genuine document, which can be caught by sophisticated verification systems.
    - ✓ Image compression analysis: Systems check for signs of image manipulation by analyzing compression artifacts.
    - ✓ Pixel-level analysis: Advanced algorithms perform detailed examinations of pixel arrays to identify modified principal components.

2. Database Verification of Personal Information provided by the signer

- Description: checking that information an end user provides about themselves - such as name, date of birth, etc. - matches a record in a known database, and that at least some of the records tie the person to the property.

- Potential actions to verify:
  - Verification of claimed personally identifiable information (PII) against credit bureaus, government agencies, and other authoritative databases. Recommended elements to verify include:
    - ✓ First Name
    - ✓ Last Name
    - ✓ Address
    - ✓ Phone Number
    - ✓ Date of Birth
    - ✓ Social Security Number (or national ID if outside of US)
  - Watchlist screening and compliance checks

  Unless otherwise required, there is no need to disclose the databases being utilized to persons being verified or persons involved in the transaction.

3. Personal Contacts and References received from the signer

- Description: Ensure that the reference sources the signer claims to have can corroborate the signer's information
- Potential Actions to Verify:
  - Independently search and obtain contact information for the reference
  - Send letter to the reference using the reference's publicly available address
  - Contact signer's real estate agent, attorney, mortgage lender, and/or accountant

4. Biometric Verification for the signer

- Description: In situations where the signer is remote, it may be helpful to determine whether the person presenting the ID is the rightful owner using physical attributes, such as requesting a "selfie" to compare against the ID.
- Potential actions to verify:
  - Facial comparison between selfie and photo ID
  - Liveness detection – preventing spoofing attempts and/or deepfakes by requesting that remote individuals follow action commands (e.g., turn left, turn right, raise your hand)

5. Use of open-source personal information to verify signer

- Description: Determine whether the provided phone number, email address and photo are likely to be those of the person who should be the signer.
- Recommended actions to verify:
  - Public search of email addresses, phone numbers, and photos. This may be used to verify if the phone number and email address have been associated with the individual's name and address in public records or commercial databases. Compare these items to information presented by the person.

- Domain Validation: Checks the validity of the email domain.
- Syntax Check: Ensures the email address follows proper formatting.
- Disposable Email Detection: Identifies temporary email addresses that have not previously been associated with the individual or represents a recently created email address.

General Recommendations

Use a layered approach that does not rely on one factor

1. Don't use knowledge based authentication (KBA) questions as a sole reliable verification
2. Don't use publicly available sources as the only source
3. Use multiple sources of verification
4. Higher risk transactions command higher vigilance

Common Fraud Indicators

1. Geographic mismatches
2. Multiple verification attempts
3. Unusual transaction timing or rush requests
4. Refusal to comply with identity verification requests
5. Abandoned identity verifications

Common Transactions targeted by impersonators

1. High-value transactions
2. Vacant lots, second home transactions, or other non-owner occupied transactions.
3. Remote closing

Employee Training

Conduct regular employee training on items including:

- Current impersonation schemes and red flags
- Advanced document forgery detection
- Social engineering tactics used by fraudsters
- Behavioral indicators of fraudulent activity

Escalation Procedures

Create escalation procedures if fraud is suspected:

- Establish documented protocol(s) for if identity fraud is suspected or concerns exist, including when and who to escalate the matter to.
- Response procedures if concerns are verified
    - Immediate response procedures for compromised identities
    - Notify local or federal law enforcement and respective fraud units
    - Develop communication protocols for affected parties. Implement immediate transaction and funding hold procedures when fraud is suspected

Additional Resources

DEFINITIONS:

Identity Proofing: The collective process of mixing and matching verifications to achieve sufficient assurance that an individual is indeed who they claim to be with the goal of tying digital identities to physical identities.

- Identity Proofing involves collecting and validating identity-related information to establish a person's identity before they can access services or complete transactions. Identity Proofing focuses on the authenticity of data provided during the onboarding or account creation processes.

Identity Verification: The process of confirming that the person presenting an identity (including a government issued ID) is the rightful owner of that identity.

- Identity verification can involve various methods, such as device intelligence, knowledge-based authentication (KBA) questions, biometric verification and multi-factor authentication (MFA).

WEBSITES:

- Experian - https://www.experian.com/business/solutions/identity-solutions/identity-verification-solutions
- National Institute of Standards and Technology (NIST) – US Department of Commerce - https://pages.nist.gov/800-63-3-Implementation-Resources/63A/verification/
- Transunion - https://www.transunion.com/faq/identity-verification
- ALTA's Seller Impersonation Page: https://www.alta.org/business-operations/operations/seller-impersonation-fraud
- ALTA Marketplace – Industry Vendors: https://www.alta.org/marketplace *
- ALTA Marketplace – "Fraud Prevention" list: https://www.alta.org/marketplace/results?code_valueList=FraudPrev *

** A vendor provider or service provider being listed or found in the ALTA Marketplace does not indicate that the providers have been vetted by ALTA; further, the applicable categories are self-reported by the providers.*

ALTA advises that your vetting of any provider's product or service should include, among others, applicability, contractual terms, risk mitigation, data protection, change management, and provider performance. These are some, but not all, of the critical components of vendor selection that a company should analyze in selecting any vendor.

Wisconsin Solo & Small Firm Conference 2025
Navigating Deepfake Technology
Cherly (Cheri) A. Hipenbecker, Knight Berry Title, Inc. & Prof. Derek Riley, Ph.D., Milwaukee School of Engineering
Additional Resources

Proof – The Trust Ledger: Transaction & Identity Fraud Bulletin

Federal Bureau of Investigation - Internet Crime Report 2024

CERTIFID – State of Wire Fraud Report 2025

Northwestern's Kellogg School of Management - Detect Fakes

METAPHYSIC – generative AI platform for photorealistic, Hollywood-grade content