

Seeing Is Deceiving:
Deepfakes, Creative Power, and the New Trust Crisis

Brian Willis, QSA, CISSP, ISO 27001 LA

Partner, LBMC

Kyle Hinterberg, QSA, CISSP, CISA

Sr. Manager, LBMC





Agenda

- Deepfakes and PCI
- AI & the New Reality
- Deepfakes 101
- Risks
- Laws & Regulations
- Detection & Defense
- Key Takeaways



Deepfakes and PCI

A convincing face or familiar voice could:

- Impersonate a customer, employee, executive, or service provider
- Social-engineer access or bypass identity-verification processes
- Request account changes, refunds or payment redirection.





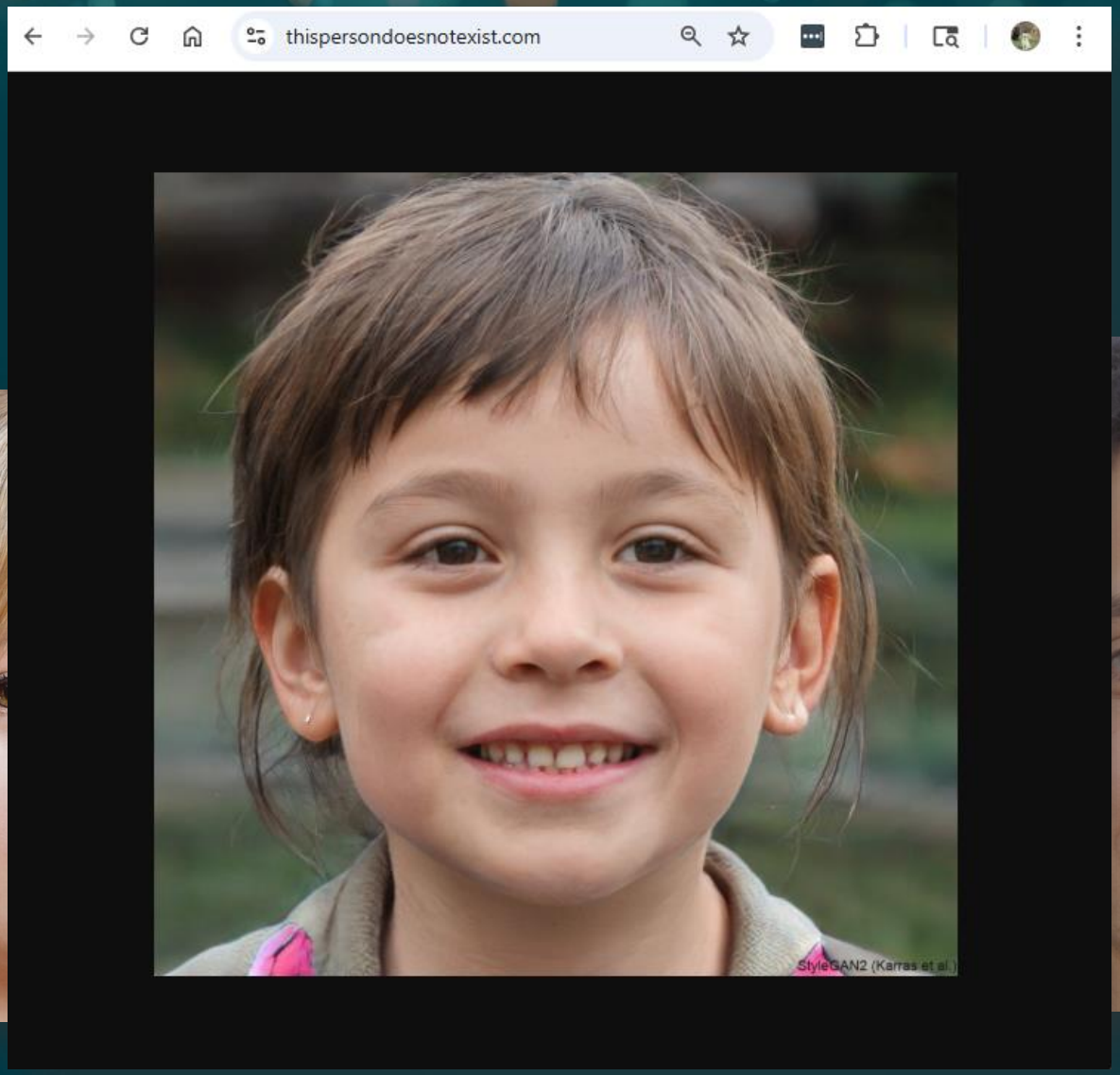


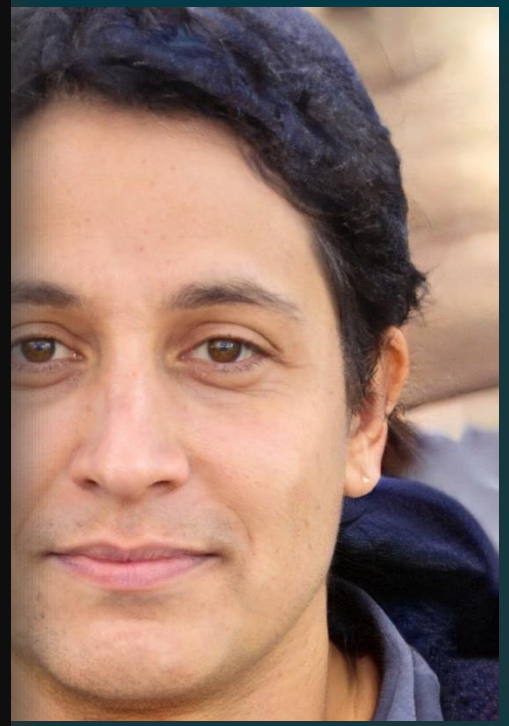
20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Real or Fake?



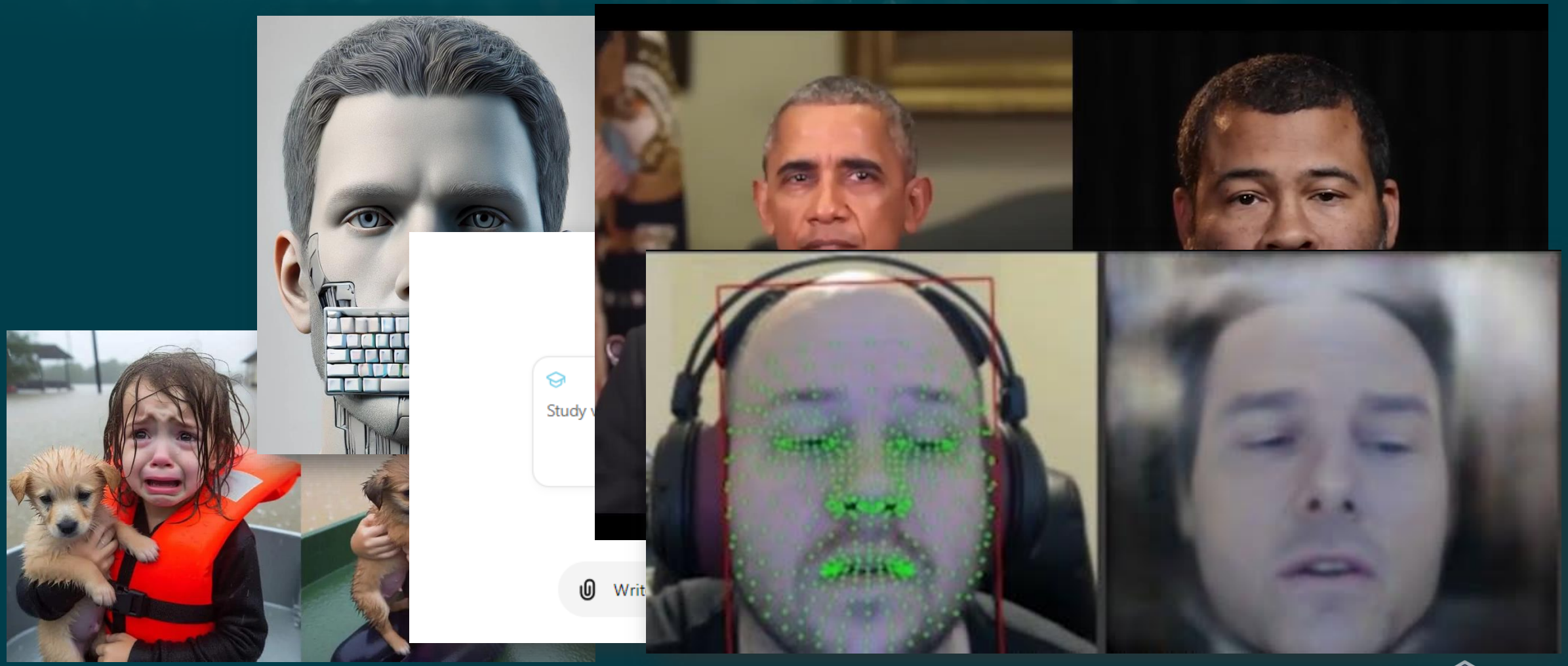






20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Deepfakes Defined



20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

“We are entering a new era where the line between reality and fiction is becoming increasingly blurred. Deepfakes are just the beginning of this revolution.”

Nina Schick, Author of "Deepfakes: The Coming Infocalypse”

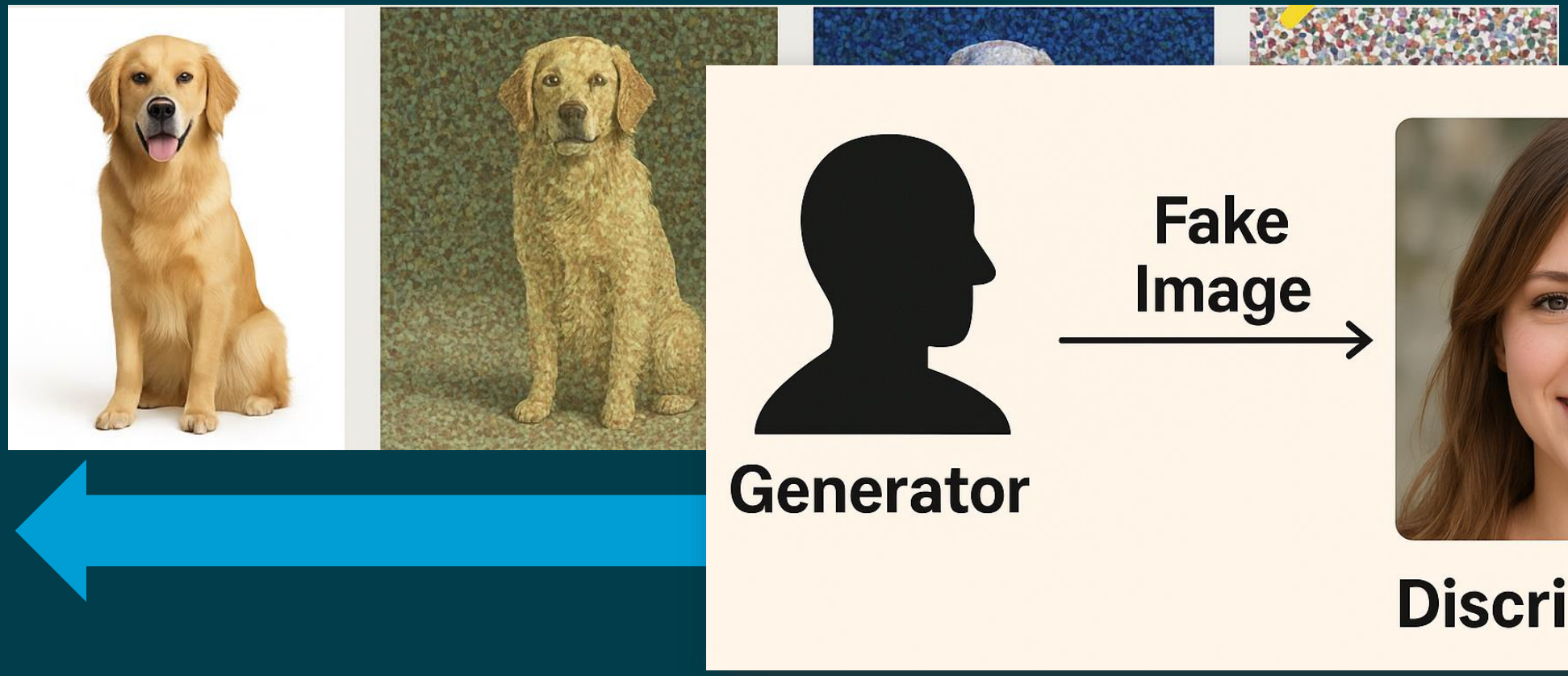


Seeing or hearing someone is no longer sufficient proof of identity or authorization.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Deepfakes Defined: Training vs. Generation

Training



Will Smith Eating Spaghetti – 2023



Source: Roy Cassette, YouTube, April 1, 2023

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Will Smith Eating Spaghetti – 2024



Source: AIGener8, YouTube, September 4, 2024

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Will Smith Eating Spaghetti – 2025



Source: Ababiya Worku, 2025

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Will Smith Eating Spaghetti – 2026



Source: radiant hole, YouTube, February 10, 2026

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Deepfakes 101



20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Deepfakes 101

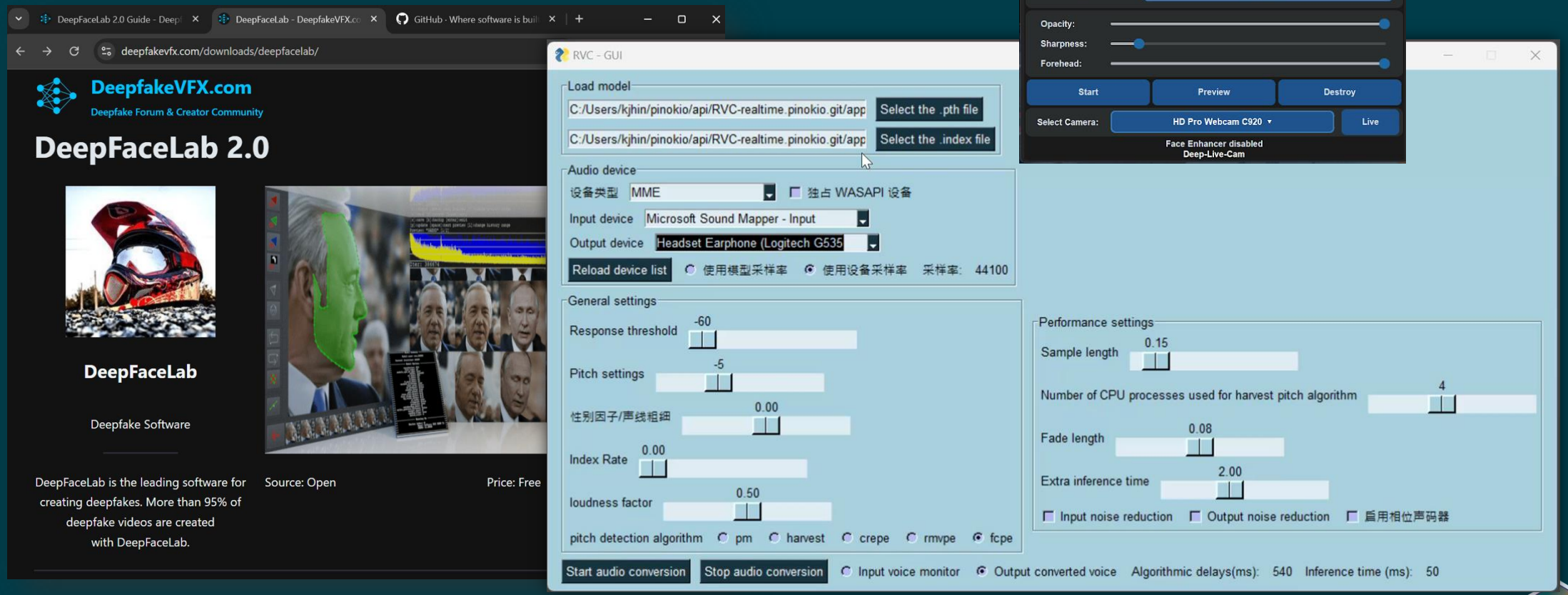
Kling AI



20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Deepfakes 101

Eleven Labs



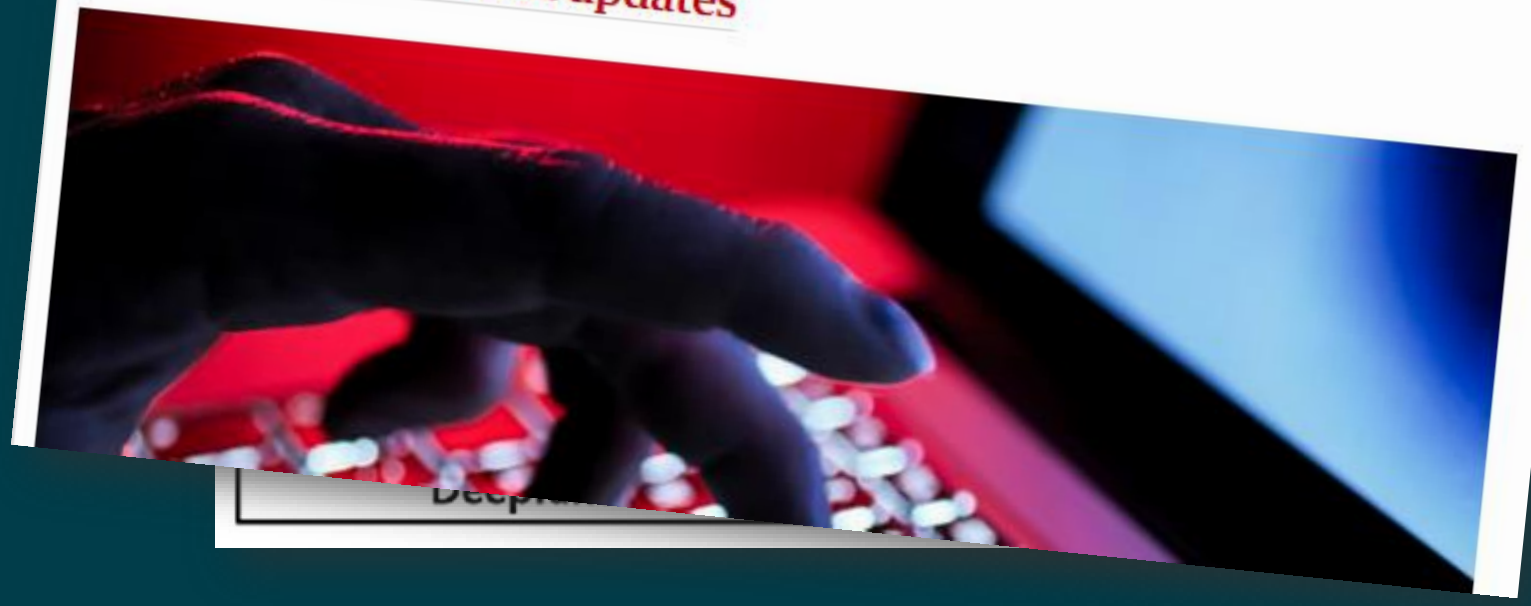
20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Deepfake Dilemmas

UK engineering firm Arup falls victim to £20m deepfake scam

Hong Kong employee was duped into sending cash to criminals by AI-generated video call

Business live – latest updates



20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Deepfake Dilemmas



Nova Scotia

How police tracked down suspects in AI deepfake investigation involving dozens of women

Court documents show how the Ottawa police used Airbnb records to unravel th

Influencer Sues Underwear Company Empowered By You Over Deepfake

June 10, 2026, 11:51 AM CDT

Nino Paoli
Reporter

Deepfakes of Nigel Farage fighting Andrew Bailey prompt scam warning

AI-generated videos depict the Reform UK leader in brawl with Bank of England governor

Mark Sellman, Technology Correspondent

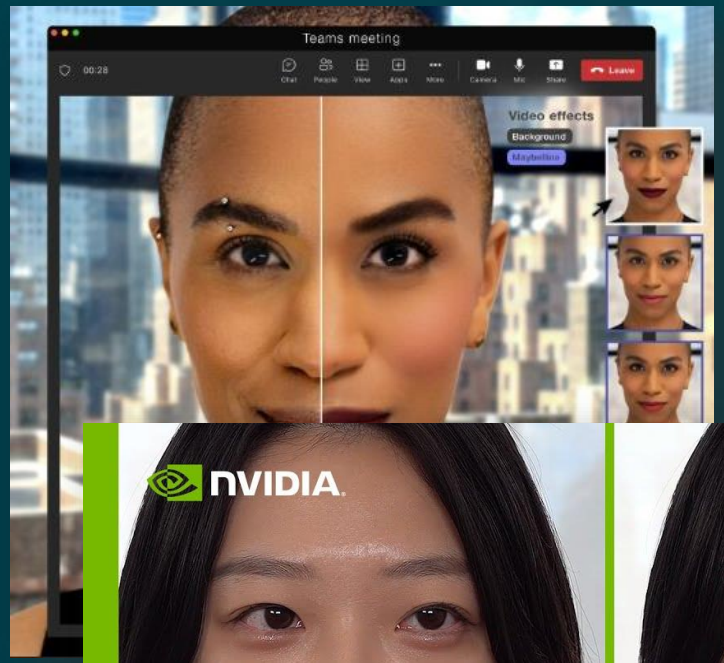
Tuesday June 09 2026, 5.00pm BST, The Times

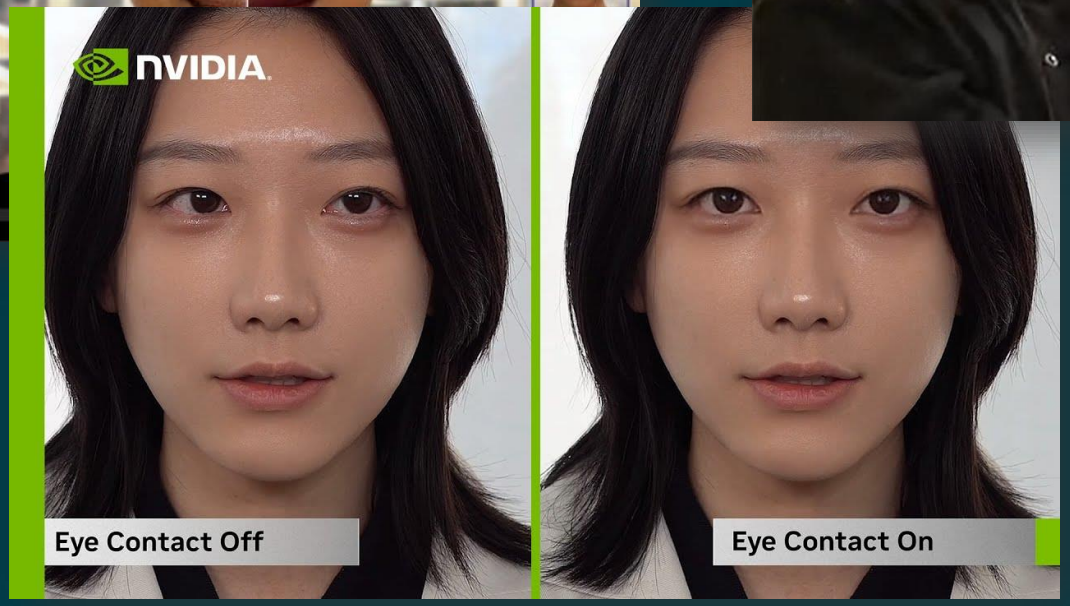
Sand Springs Public Schools investigating deepfake photos of administrators sent through student email

FOX23.com News Staff Jun 10, 2026 Updated 2 hrs ago

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Beneficial Deepfakes







‘Being on camera is no longer sensible’: persecuted Venezuelan journalists turn to AI

Journalists are using artificial intelligence avatars to combat Maduro’s media crackdown since disputed election



The AI newsreaders La Chama and El Pana have been providing daily updates on the Venezuelan president’s post-election crackdown. Photograph: Connectas

OF SECURING
MENT DATA

Deepfake Law:
The Trend is Clear, the Map is Messy

Legal categories to track:

- Intimate-image abuse
- Election and political synthetic media
- Voice, likeness, and creator-rights protections
- Platform takedown and transparency obligations



20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

US Federal

Law	Year/Status	Primary Goal
IOGAN Act	Enacted 2020	managing synthetic or
DEEPFAKE Accountabil		ain deepfakes and
DEFIANCE		nsual sexually explicit
NO FAKES		nauthorized digital
Deepfake Re / FY2021 ND 9004		/deepfake threats.
TAKE IT DOWN Act	Enacted 2025; active 2026	Criminalizes nonconsensual intimate visual depictions and requires covered platform takedown processes.



20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

US States (non-exhaustive)

Law	Jurisdiction	Year	Primary Goal
AB 2355	California	2024	Requires AI disclosure in certain political advertisements.
AB 602 / AB 621	California	2019 / 2025	Creates and expands civil remedies for nonconsensual sexually explicit deepfakes.
ELVIS Act	Tennessee	2024	Protects voice, image, and likeness from unauthorized AI/synthetic replication.
Act 123	Wisconsin	2024	Requires disclosures when certain political ads use audio or video substantially produced by generative AI.
HB 591	North Carolina	2024	Expands sexual extortion, intimate-image, and child-exploitation laws to cover AI-generated or computer-generated depictions.
H.3058 / S.28	South Carolina	2025	Penalizes unauthorized disclosure of digitally forged intimate images and criminalizes AI/computer-generated child sexual abuse representations.

20 YEARS OF SECURING PAYMENT DATA PCI Security Standards Council

US States (non-exhaustive)

Law	Jurisdiction	Year	Primary Goal
SB 751	Texas	2019	Early election deepfake law; criminalizes certain deceptive political deepfake videos near elections.
SB 1361 / SB 441	Texas	2023 / 2025	Criminalizes production or distribution of sexually explicit deepfake media.
Chapter 58 / HF 1370	Minnesota	2023	Covers both election deepfakes and nonconsensual deepfake sexual images through civil and criminal remedies.
SB 5152 / HB 1999	Washington	2023 / 2024	Requires election synthetic-media disclosures and criminalizes fabricated intimate images.
HB 1133 / HB 1047	Indiana	2024	Requires disclaimers for fabricated election media and expands intimate-image law to AI/computer-generated images.
SB 5959	New York	2020; effective 2021	Protects postmortem digital-replica rights and provides a private action for certain sexually explicit deepfake depictions.

20 YEARS OF SECURING PAYMENT DATA PCI Security Standards Council

International (non-exhaustive)

Law	Jurisdiction	Year/Status	Primary Goal
Deep Synthesis Provisions	China	2023	Regulates deep synthesis services; requires labeling, user controls, and restrictions on harmful or misleading synthetic content.
AI Act	European Union	Enacted 2024; phased compliance	Requires transparency for AI-generated content, including labeling/disclosure of deepfakes and certain synthetic media.
Digital Services Act	European Union	Fully applicable 2024	Requires platforms to assess and mitigate risks, including illegal content, disinformation, election risks, and gender-based harms.
Online Safety Act / Data Use and Access Act	UK	2023 / 2025; active 2026	Criminalizes sharing, threatening to share, creating, or requesting non-consensual intimate deepfake images.
Public Official Election Act amendment	South Korea	2023	Bans AI deepfake campaign content during the 90-day period before elections.
Sex Crimes Act deepfake amendments	South Korea	2024	Criminalizes creation, distribution, possession, and viewing of non-consensual sexually explicit deepfakes.

20 YEARS OF SECURING PAYMENT DATA PCI Security Standards Council

Methods Used by Deepfake Detection Tools



- Inconsistencies in Facial Artifacts
- Audio-Visual Mismatch
- Pixel-Level Analysis
- Motion Analysis
- Metadata and Hash Analysis
- Gaze and Eye Movement Analysis
- Shading and Lighting Discrepancies
- Temporal Artifacts
- Biometric Feature Consistency

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council





DeepFake-O-Meter

University at Buffalo

NSF National Science Foundation

https://zinc.cse.buffalo.edu/ubmdfl/deep-o-meter/

20 YEARS OF SECURING PAYMENT DATA

DeepFake-O-Meter



Detector	Result	Details
AVSRDD (2025)	100.0% AI-Generated Likelihood	View detail
AltFreezing (2023)	66.2% AI-Generated Likelihood	View detail
CFM (2025)	48.9% AI-Generated Likelihood	View detail
DSP-FWA (2019)	14.9% AI-Generated Likelihood	View detail
FTCN (2021)	0.2% AI-Generated Likelihood	View detail
LIPINC (2024)	100.0% AI-Generated Likelihood	View detail
LSDA (2024)	50.6% AI-Generated Likelihood	View detail
SBI (2022)	26.2% AI-Generated Likelihood	View detail
TALL (2023)	100.0% AI-Generated Likelihood	View detail
WAV2LIP-STA (2022)	85.7% AI-Generated Likelihood	View detail
XCLIP (2022)	43.8% AI-Generated Likelihood	View detail

DeepFake-O-Meter

MEDIA PREVIEW



Resolution: 1280 × 720 Format: MP4 File Size: 1.89MB Open media

OVERALL SYSTEM ASSESSMENT

Likely Authentic

CONFIDENCE

Moderate

Moderate signal strength

Image Detectors

Not Applicable

Video Detectors

2 High · 1 Moderate · 8 Low

Audio Detectors

Not Applicable

20 YEARS OF SECURING PAYMENT DATA PCI Security Standards Council

Methods Used by Deepfake Detection Tools



Issues

- Availability
- False Positives

Do we need to reconsider using an individual's likeness as a primary identifier?

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Deepfakes And PCI

INFORMATION SUPPLEMENT: Authentication Guidance

Best practice 2: Implement controls to mitigate deepfake attacks.

- Deepfakes can defeat video and voice verification.
- Reassess authentication controls for impersonation risk.
- Use supplementary signals for added assurance:
  - Device or computer ID
  - Location
  - Operating system
  - Access time or type
  - Typing behavior



**Supplementary signals do not independently satisfy PCI DSS MFA requirements.*

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

What Can We Do? – Identification

mit media

Voice clones sound realistic but not (yet) hyperrealistic

https://www.eurekalert.org/news-releases/1099494

- The study did not find a "hyperrealism effect" in AI voices
- AI voices now indistinguishable from real human speech
- Often judged more dominant and sometimes more trustworthy than humans
- Voices were created with minimal audio and common tools
- **Published September 24, 2025**

they can

- People
- People are highly
- **Published October 29, 20**

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

What Can We Do? – Identification

Social Engineering Awareness

- Urgency or Pressure
- Unusual Requests for Personal Information
- Emotional Manipulation
- Unexpected Communication
- Requests for Money or Financial Tra
- Inconsistencies in Communication
- Unfamiliar Links, URLs, Addresses
- Impersonation of Authority
- Too Good to Be True Offers
- Unusual Behavior from Familiar Co

12.6.3.1 Security awareness training includes awareness of threats and vulnerabilities that could impact the security of cardholder data and/or sensitive authentication data, including but not limited to:

- Phishing and related attacks.
- Social engineering.



Deepfakes make deception easier.

Strong controls make it less effective.

Thank you!

Visit us at Booth #29



LBMC

Brian Willis, QSA, CISSP, ISO 27001 LA
brian.willis@lbmc.com
linkedin.com/in/brianswillis

Kyle Hinterberg, QSA, CISSP, CISA,
kyle.hinterberg@lbmc.com
linkedin.com/in/kylehinterberg