

# IDENTITY THEFT & IMPERSONATION REPORT

Subject: Criminal Identity Theft, AI-Based Voice Impersonation, and Digital Exploitation by Mr. Danny de Hek

1. COMPLAINANT DETAILS Name: Mr. Shavez Ahmed Siddiqui alias "Shavez"  
Position: Chief Executive Officer Organization: Lquidpay DEO Bank Location: Dubai, UAE Email: shavez@lquidpay.finance
2. RESPONDENT DETAILS Name: Danny de Hek Known Aliases: "Crypto Avenger," "Scam Patrol," etc. Digital Platforms Used: YouTube, Shorts, Instagram, LinkedIn, Reddit, BuyMeACoffee, X (formerly Twitter), Rumble, Bloomberg.com Hosting Provider of Website (dehek.com): WPengine.com Additional Malicious Domain: [www.lquidpay.com](http://www.lquidpay.com) – This website, created and maintained by Mr. Danny de Hek, fraudulently impersonates Lquidpay DEO Bank and includes defamatory content falsely labeling the complainant and the organization as a scam. The content also embeds a Bloomberg video from its official YouTube channel that defames Mr. Shavez Ahmed Siddiqui and Lquidpay DEO Bank. As such, both Bloomberg Media and its reporter Alice Kantor are equally responsible for disseminating defamatory, misleading, and unauthorized material. The website is hosted at IP address 141.193.213.21 (IP range: 141.193.213.0–141.193.213.255, CIDR), under the ISP Cloudflare London, LLC, and its organization listed as WPengine, Inc.

Registrar Information: Registrar: eNom, LLC WHOIS Server: whois.enom.com  
Referral URL: <http://www.enomdomains.com>

Important Dates: Created: 12/25/2024 Updated: 03/12/2025 Expires: 12/25/2026

Nameservers:

- ns1.1stdomains.net.nz (162.159.26.245)
- ns2.1stdomains.net.nz (162.159.27.184)

This constitutes identity theft, brand misuse, and coordinated online defamation, warranting immediate legal and platform-level action. Additionally, the domain provider (eNom, LLC), hosting services (WPengine, Inc.), and content partners—namely Bloomberg Media and reporter Alice Kantor—are held equally accountable for enabling the publication and persistence of malicious, defamatory, and impersonating content. Their failure to moderate and remove such harmful material, despite its clear potential to incite widespread public misinformation and mental trauma, makes them complicit. The sustained publication of such content

nearly resulted in life-threatening harm to Mr. Shavez Ahmed Siddiqui, and thus their legal liability must be evaluated with utmost seriousness.

3. **INCIDENT SUMMARY** This report documents a deliberate and criminal act of identity theft and impersonation carried out by Mr. Danny de Hek against Mr. Shavez Ahmed Siddiqui, CEO of Lquidpay DEO Bank. The respondent has unlawfully used artificial intelligence (AI) tools and voice synthesis technologies to fabricate audio and video materials mimicking the complainant's voice and likeness.

Furthermore, Bloomberg Media and its reporter Alice Kantor are equally implicated, as their official content—embedded on the impersonating domain [www.lquidpay.com](http://www.lquidpay.com)—reinforces and amplifies the defamatory claims initiated by Mr. Danny de Hek. The hosting provider WPEngine, Inc., and domain registrar eNom, LLC also bear responsibility for continuing to allow this content to remain online despite its clear potential for reputational and psychological harm. Their combined actions and negligence nearly resulted in a fatal outcome for Mr. Siddiqui, underscoring the urgent need for multi-jurisdictional accountability.

Specific allegations include:

- **AI-Generated Voice Cloning:** Unauthorized creation and circulation of AI-generated voice clips impersonating Mr. Siddiqui, without consent, across public platforms.
- **Fake Video Content:** Dissemination of deepfake videos intended to mislead audiences by simulating Mr. Siddiqui's speech and behavior, presented as authentic.
- **False Representation:** Misuse of Mr. Siddiqui's identity in content titles, thumbnails, and social posts portrays him as a criminal without a legal basis or authority.
- **Violation of Personal Privacy:** Use of AI tools to synthesize personal and private content designed to manipulate public perception and falsely implicate Mr. Siddiqui.
- **Misuse of Business Identity and Brand Assets:** Unauthorized use of Lquidpay Deobank's logo, trademarks, and visual identity—including that of other affiliated ventures—to falsely represent, defame, and misguide the public through manipulated video posts, misleading articles, and defamatory media content.
- **Misuse of Personal Images:** Use of Mr. Siddiqui's photographs without consent in defamatory and misleading content, designed to exploit his image and misguide the audience for malicious purposes.

#### 4. CONSEQUENCES OF IDENTITY THEFT

- **Emotional and Psychological Trauma:** The impersonation triggered panic attacks, anxiety, and trust issues, compounding the stress leading to a medically verified brain stroke. [Annexure 1: Health Report]
- **Damage to Credibility:** Stakeholders, clients, and investors questioned the authenticity of leadership communications, harming Liquidpay Deobank's public trust.
- **Security Threat:** Unauthorized use of personal voice and image data poses ongoing cybersecurity risks to Mr. Siddiqui and Liquidpay Deobank's brand.
- **Business Disruption:** Operational confusion and miscommunication resulted in failed contracts, damaged relationships, and financial losses.

5. EVIDENCE ATTACHED Audio Comparisons: Authentic vs AI-generated voice samples 🔗 Links to impersonated videos and deepfake content 📄 Character Certificate: Officially issued by police authorities confirming Mr. Shavez Ahmed Siddiqui has no criminal record. This directly contradicts the AI-generated audio created by Danny de Hek, in which Mr. Siddiqui was falsely made to state that he was jailed.

#### 6. APPLICABLE LEGAL VIOLATIONS 🇮🇳 India

- Information Technology Act, 2000 (Sections 66C & 66D - Identity Theft and Impersonation)
- IPC Section 499 – Defamation
- IPC Section 500 – Punishment for Defamation

#### 🇦🇪 UAE

- Federal Law No. 34 of 2021 – Articles 10 & 44: Cyber Identity Fraud

#### 🇺🇸 United States

- Computer Fraud and Abuse Act; State-based impersonation laws

#### 🇳🇿 New Zealand

- Crimes Act 1961 – Section 252 (Accessing computer systems for dishonest purposes)

#### 🇬🇧 United Kingdom

- Communications Act 2003 – Section 127: Improper use of public electronic communications network

- Malicious Communications Act 1988 – Section 1: Sending letters or other communications with intent to cause distress or anxiety
- Defamation Act 2013 – Protection against serious harm to reputation

7. LEGAL DEMANDS & FINAL NOTICE You are hereby directed to:

- Immediately remove all impersonated and AI-generated content.
- Issue a public clarification and apology on all affected platforms.
- Cease all current and future attempts of identity misuse.

Failure to comply within 7 working days will result in:

- Criminal complaints and FIRs across India, UAE, USA, and New Zealand.
- Litigation against content platforms enabling impersonation.
- Claims for damages and injunctive relief.

8. DECLARATION I, Shavez Ahmed Siddiqui, hereby declare the information provided above to be accurate and truthful. I reserve full rights to pursue legal action against all parties responsible for identity theft and impersonation. This includes but is not limited to Danny de Hek, Alice Kantor, Bloomberg Media, the domain registrar eNom, LLC, and hosting provider WPENGINE, Inc.—each of whom has enabled, permitted, or contributed to the creation and public dissemination of malicious, defamatory, and impersonating content that posed a threat to my life, safety, and professional reputation.

Date: [Insert Date] Place: Lucknow, India Signature:

---

9. ANNEXURES

Annexure A – Audio Comparison Files

[AI generated tampered voice](#)

Transcript of alleged audioShavez (Tampered Voice)

I'm surprised that you've dug up my history. Yes, it's true that I spent five years in prison in India for fraudulent activities. However, since my release, I've made a conscious effort to change and avoid repeating past mistakes. While I understand your concern about my background and its potential impact on my ability to run a business in the financial services sector, I can assure you that I've learned from my past errors and am committed to conducting business ethically and transparently. I hope this explanation provides clarity on your question.

Danny

(beep) Does provide me clarity, but it does actually wave a few red flags. For example, if you're being released at a prison, normally you're on bail conditions. Have your conditions not, uh, uh, uh... Are your bail conditions allowing you to run a company and control finances once again, or isn't that a breach of bail conditions?

**The AI-generated voice falsely claims that Mr. Shavez Ahmed Siddiqui has been jailed — a completely fabricated narrative.**

**As validated in Annexure C, Mr. Siddiqui holds a clean character certificate with no criminal record or history of incarceration.**

Shavez (Tampered Voice)

(beep) It's important to clarify that my incarceration...

[Real Voice](#) ( A legit work meeting where shavez is speaking )

Annexure B – [Image and Video URLs of Defamatory Content](#)

Annexure C – [Character Certificate](#)