Event Report

CloudSEK

ForgeCraft : Unmasking a China-Linked Operation Selling Counterfeit IDs Across North America

Category

Adversary Intelligence

Region

North America

Sourajeet Majumder
Security Researcher

Ibrahim Saify
Security Researcher

info@cloudsek.com

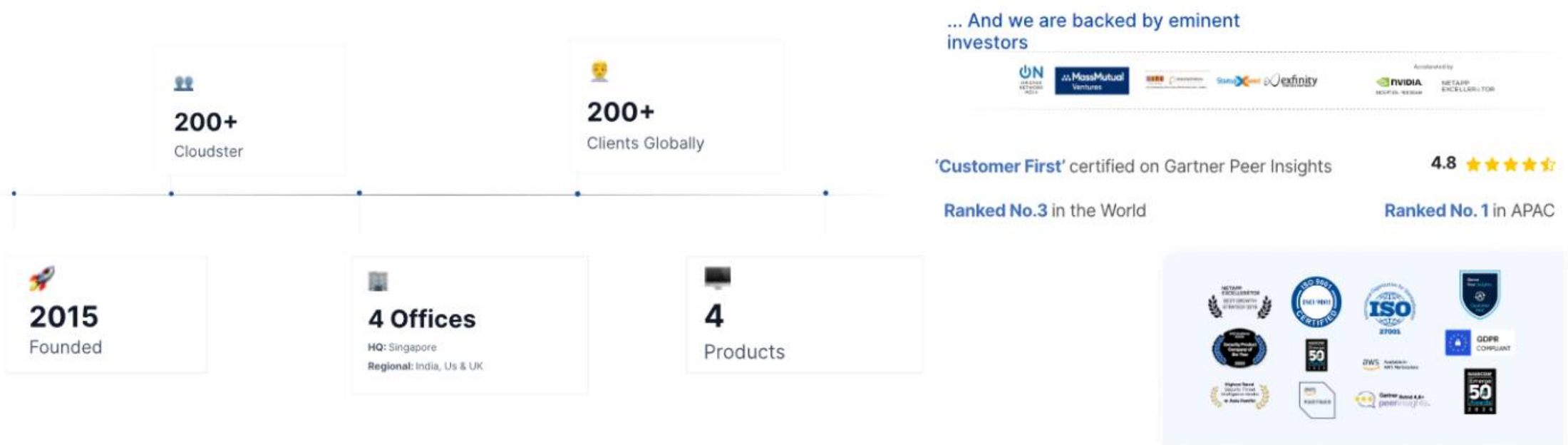
www.cloudsek.com

Table of Contents

Page No.

About CloudSEK

CloudSEK is a Cyber Intelligence company offering Predictive Threat Analytics, Digital Risk Protection, Attack Surface and Supply Chain Monitoring, helping global organizations quantify and prioritize cyber threats for robust security.



Executive Summary

A single counterfeit driver's license can unlock dangerous opportunities, ranging from **illegal firearm purchases and SIM-based fraud schemes** to **collecting stolen goods from couriers requiring ID verification**. Beyond such high-stakes threats, counterfeit licenses also enable everyday abuses like bypassing age limits for alcohol or tobacco, renting cars and hotels, securing jobs under false identities, or helping undocumented immigrants obtain counterfeit identities. Mass-produced and sold online, these IDs don't merely evade security - they actively undermine trust in legal, financial, and civic systems.

CloudSEK's STRIKE team uncovered an extensive counterfeit identity operation selling U.S. and Canadian driver's licenses (all states/provinces) and Social Security Number (SSN) cards. Our investigation traced the network to a **China-based threat actor** operating an infrastructure of 83+ interconnected domains, supported by **24/7 WeChat assistance**, custom order flows, and multiple payment channels.

Key Findings:

- **4,500+ unique buyers** identified in the exfiltrated database.
- **6,500+ counterfeit licenses** sold, with many buyers purchasing multiple IDs.
- Total estimated revenue generated by the threat actor: **$785,000+ USD.**
- Dense buyer clusters in the **U.S. Eastern Seaboard** and other **Canadian provinces**.
- Payments processed via **LianLian Pay, PayPal**, cryptocurrencies, Western Union, credit/debit cards, and more.
- **Covert packaging methods** being utilized by the threat actor to evade customs, verified through real shipment tracking.
- **Exact geolocation** and a **facial image** of the threat actor obtained via controlled HUMINT engagement.

Critically, more than **3,800 buyers were potentially found to be above the age of 25**. This signals intentions beyond casual misuse.

An investigation into one of the buyers revealed connections to two trucking and logistics companies with prior regulatory violations and revoked authorities. The same email, linked to these businesses, was used to purchase multiple fake commercial driving licenses, indicating potential systemic misuse. Such DLs could enable unauthorized drivers, bypass compliance checks, and facilitate illicit logistics or trafficking operations, posing serious risks to national security.

This whitepaper details the **tactics, techniques, and procedures (TTPs)** used - from domain setup and **shell e-commerce sites** to **marketing on Meta Ads** (along with other social media) - revealing a professionalized, scalable supply chain for fake IDs. It also outlines the operational, legal, and security risks posed by such networks, and provides recommendations for disrupting this growing national threat.

4,500+ unique buyers

6500+ Counterfeit Licenses Sold

$785,000+ Revenue Generated

U.S. East Coast & Canada Provinces

TA's Location and Face Obtained

LianLian Pay, PayPal

Infrastructure Analysis

As part of this investigation, CloudSEK researchers identified a total of **83 domains** attributed to the same threat actor. These domains are being used to facilitate the sale and distribution of fake licenses and related documents.

- While some of the domains were found to be **hosted on the same ASN**, others were **distributed across different ASNs**, indicating efforts to maintain redundancy and evade takedowns.
- A recurring domain keyword **"idcaca"** was observed, registered under multiple top-level domains (TLDs) suggesting brand consistency and wider reach.

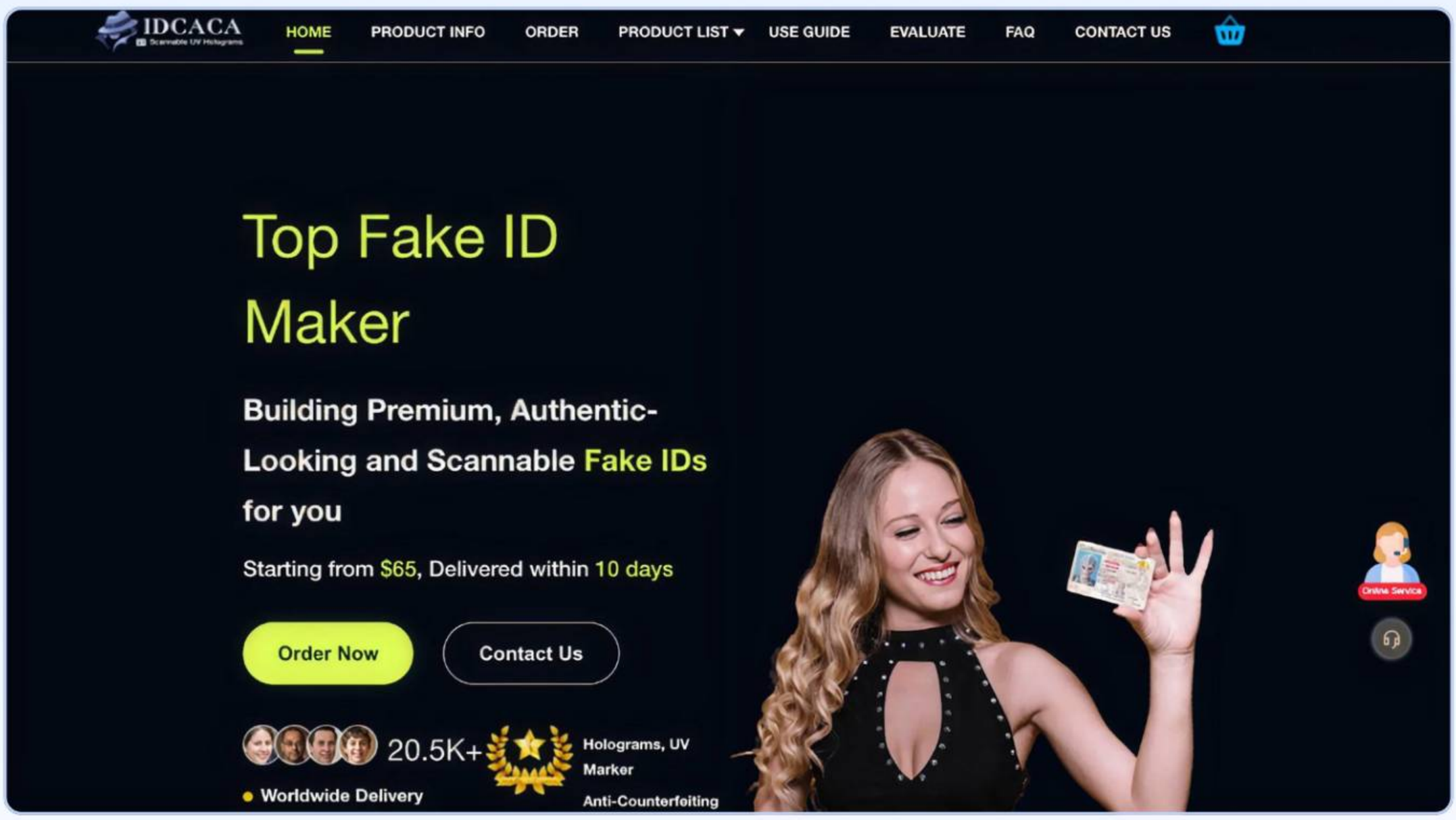
idcaca[.]com	idcaca[.]buzz	idcaca[.]online	makeidcard[.]top	idlord[.]shop	dofakeid[.]com
idcaca[.]cc	idcaca[.]cfd	idcaca[.]site	chicfinds[.]top	fakeidsellers[.]top	idreplica[.]com
idcaca[.]fun	idcaca[.]pics	idcaca[.]yachts	newyorkdl[.]shop	idpapa[.]cc	idscan[.]life
idcaca[.]ink	idcaca[.]homes	idcaca[.]beauty	pennsylvaniadl[.]shop	buyids[.]top	idsmonster[.]ph
idcaca[.]lat	idcaca[.]click	idcaca[.]bond	newyorkdl[.]top	idlord[.]org	megusta[.]top
idcaca[.]lol	idcaca[.]life	idcaca[.]qpon	pennsylvaniadl[.]top	californiaids[.]com	buyusid[.]shop
idcaca[.]mom	idcaca[.]rest	idcaca[.]quest	buyid[.]click	fakeidshops[.]com	idcards[.]top
idcaca[.]pro	idcaca[.]skin	idcaca[.]top	californiadl[.]top	fakeid724[.]com	idcola[.]top
idcaca[.]shop	idcaca[.]autos	idcaca[.]xyz	floridadl[.]top	buyidcards[.]com	makeid[.]top
idcaca[.]vip	idcaca[.]boats	idsmaster[.]com	buyusid[.]com	buyidshop[.]com	scanid[.]top
idcaca[.]art	idcaca[.]cyou	georgiadl[.]top	buyusid[.]xyz	fakeidcard[.]top	scanid[.]shop2
idcaca[.]help	idcaca[.]hair	texasdl[.]top	buyid[.]lol	superbfakeid[.]com	stateid[.]top
idcaca[.]icu	idcaca[.]makeup	proscandl[.]top	buyusid[.]lol	createidcrad[.]top	usid[.]top
idcaca[.]sbs	idcaca[.]monster	northcarolinadl[.]top	sifumu[.]shop	createfakeid[.]com	-

Snapshot displaying the 83 domains which are part of the threat actor's infrastructure

Common Website Structure

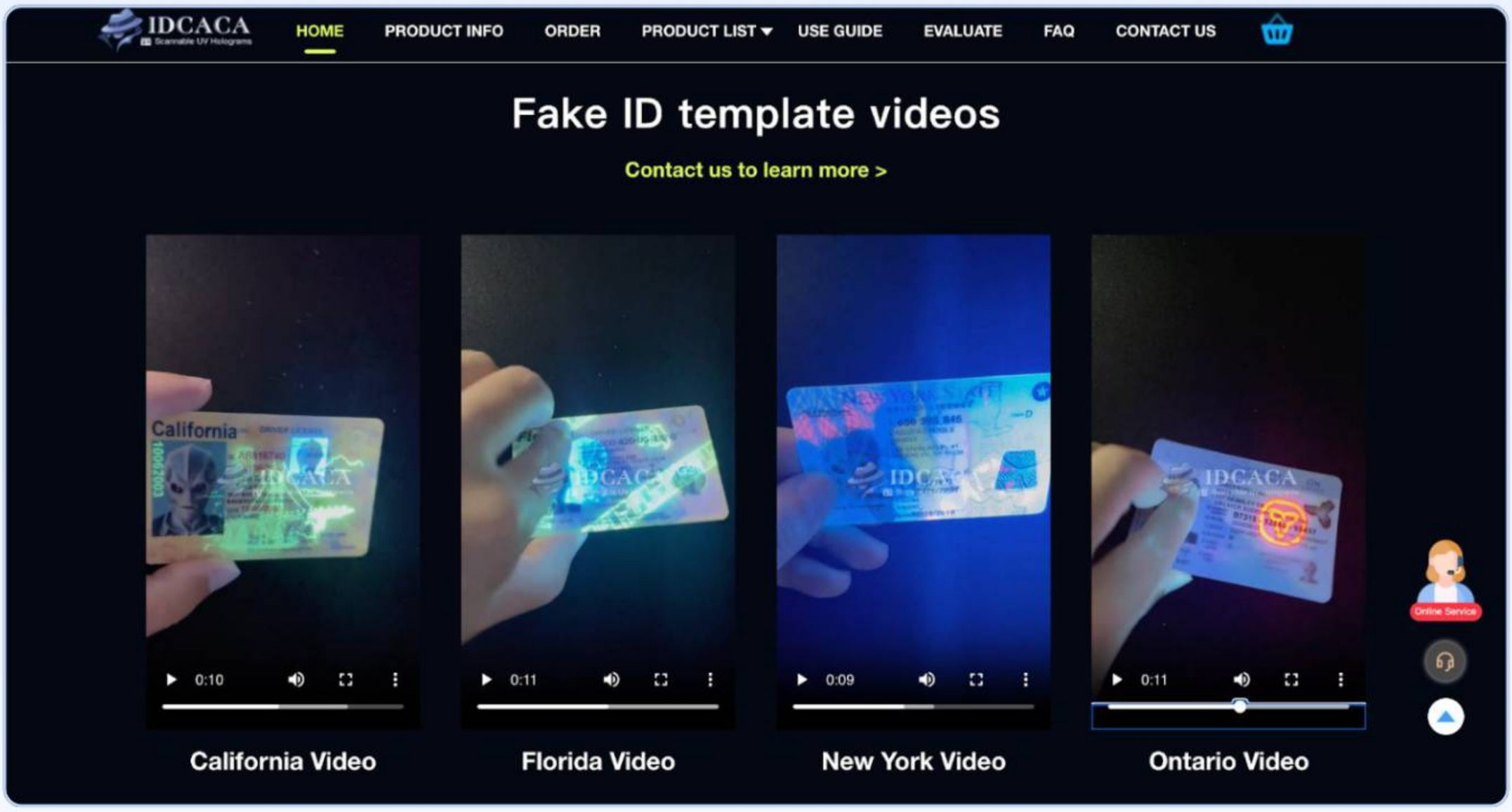
Most of these domains shared a **uniform interface and structure**, typically including the following web pages:

- **Home:** Landing page introducing the service
- **Product Info:** Details on fake license features, packaging, and shipping
- **Order:** Online form for placing orders
- **Product List:** Catalog of available documents (e.g., licenses, SSNs)
- **Use Guide:** Step-by-step instructions on placing and receiving orders
- **Evaluate:** Customer reviews and testimonials
- **FAQ:** Frequently asked questions
- **Contact Us:** Communication and support options

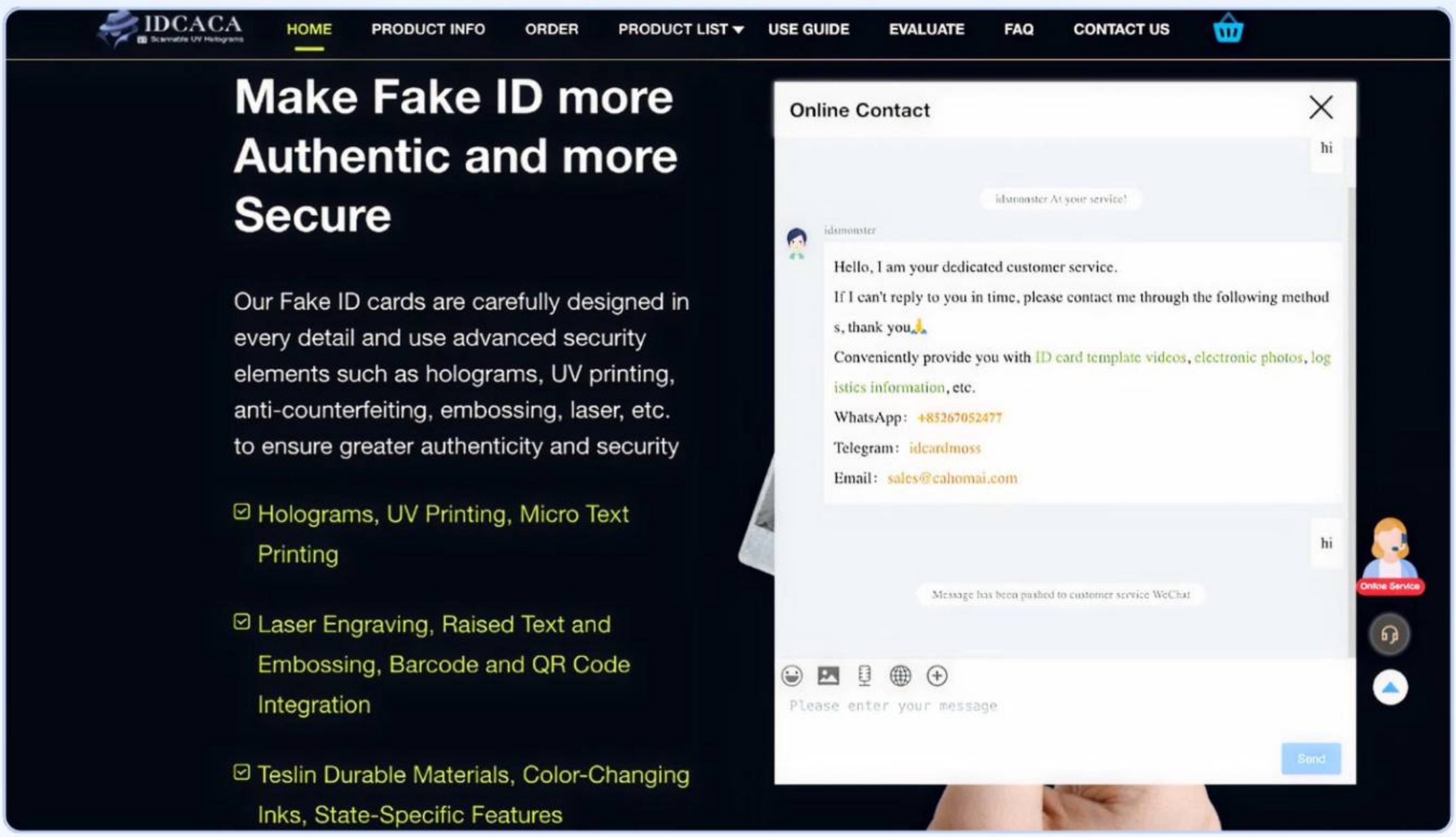


Snapshot of the home page for idcaca[.]com

Additionally, each site includes a **24/7 live support chat**, which routes communication via **WeChat**, offering real-time interaction with potential buyers.



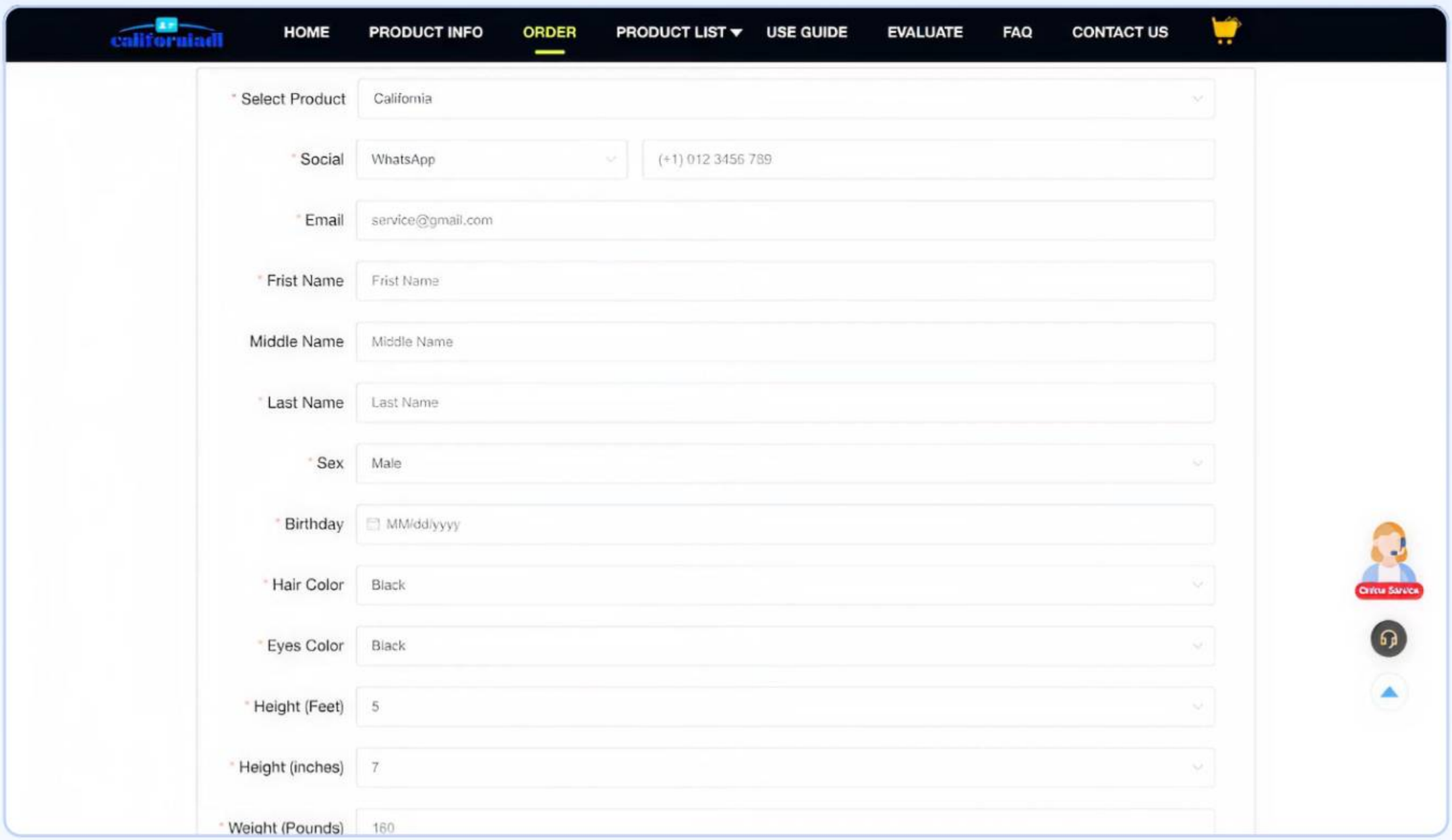
Snapshot of the home page for idcaca[.]com displaying videos of the UV feature in the fake ID cards



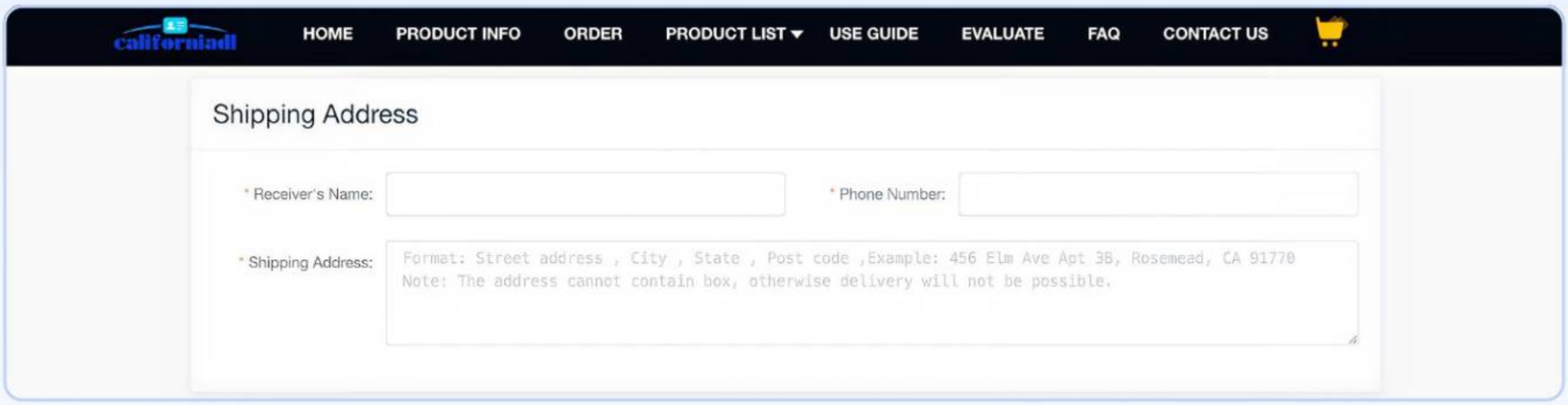
Snapshot displaying the 24×7 customer chat box powered by WeChat

One of the most critical components of the threat actor's infrastructure is the **Order Page**, which facilitates customer input and initiates the fake license purchase process. The ordering flow includes several customizable fields such as:

- **Personal details:** Name, phone number, picture, signature, physical address, height, and other user-defined data fields.
- **Shipping information:** Users must enter a delivery address and select options for expedited production or express shipping.
- **Payment options:** Customers are offered multiple payment methods to complete their purchase.



Snapshot displaying the order form

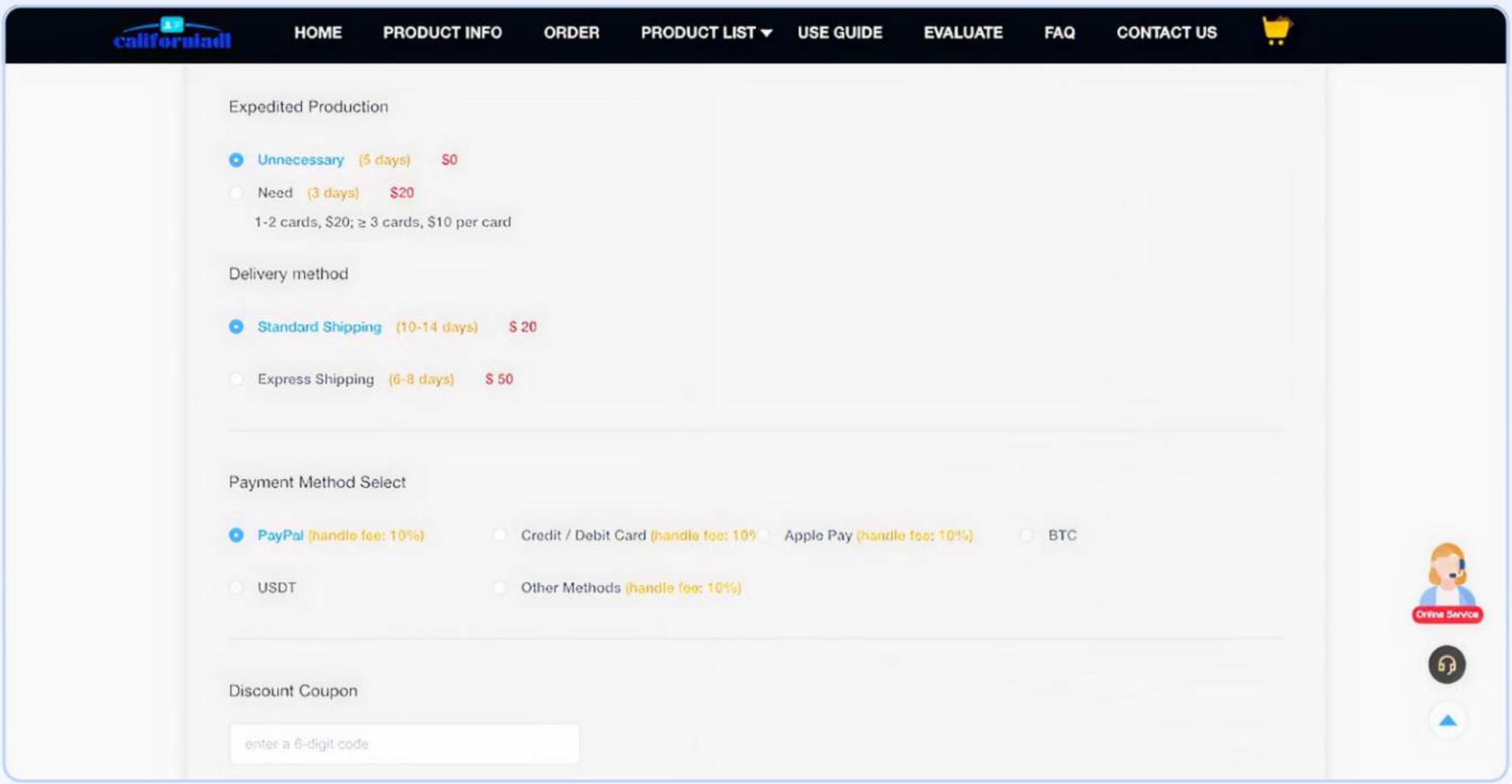


Snapshot displaying the shipping address form

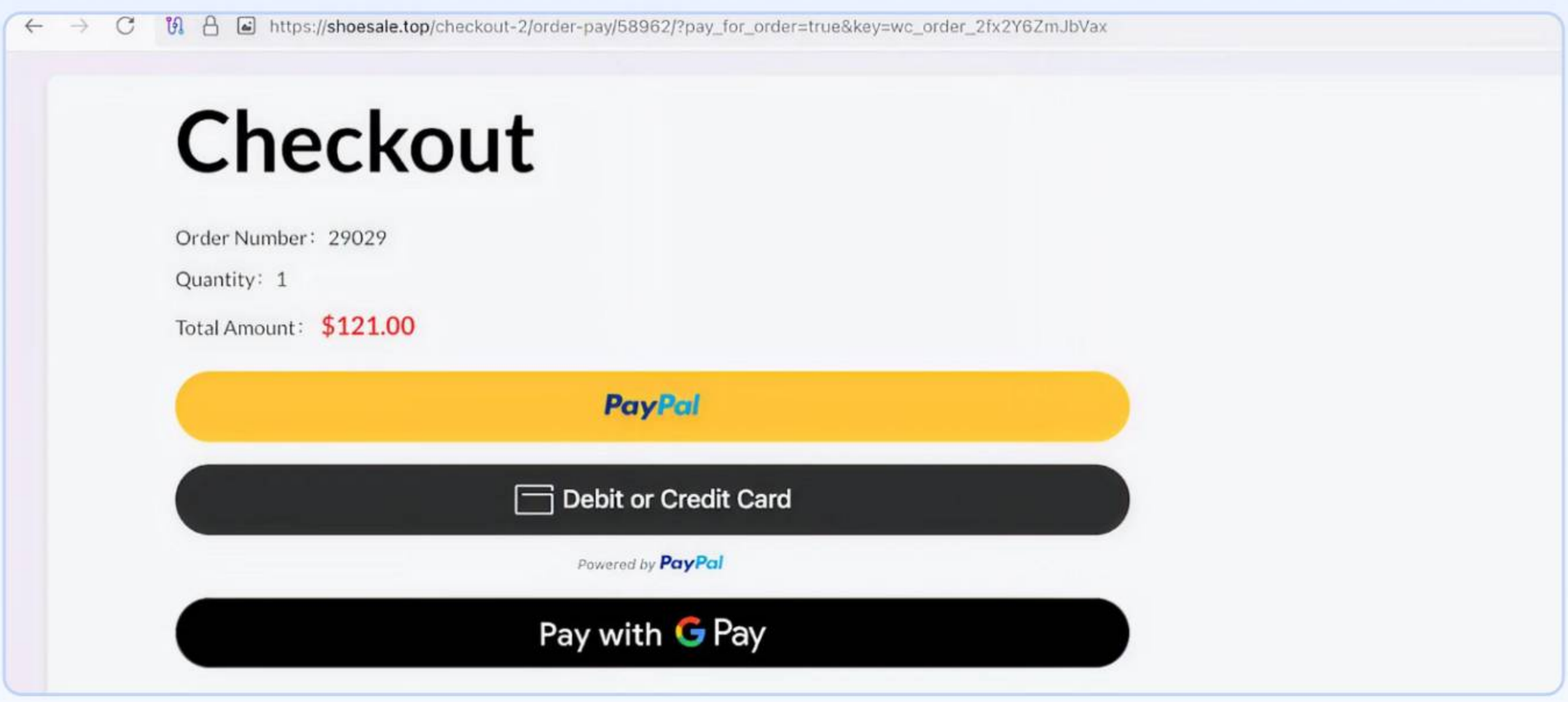
If a buyer opts for **PayPal** or **Credit/Debit Card**, they are redirected to a **WooCommerce payment gateway**. This redirection is made to multiple sites that appear to be hosted on **WordPress** and designed to mimic legitimate e-commerce platforms.

CloudSEK researchers identified several such websites that likely act as **shell companies or financial fronts**, posing as online stores for shoes, clothing, or accessories:

- accshop[.]life , cahomai[.]com, pantsale[.]top, shoesale[.]top, sifumu[.]shop



Snapshot displaying the payment methods once a buyer fills up the order form



Snapshot displaying Woocommerce payment gateway at shoesale[.]top being used for PayPal, Card payments

These sites may be used to mask transactions for fake identity document purchases, offering the threat actor a flexible and seemingly legitimate vehicle for various financial maneuvers.

Product Analysis

The counterfeit **U.S. and Canadian driver's licenses** (all states/provinces) and **Social Security Number (SSN)** cards being sold are marketed as high-quality, scannable replicas designed to mimic genuine government-issued IDs.

Pricing Structure:

- **1 unit:** $90
- **2 - 3 units:** $80 each
- **4 - 9 units:** $70 each
- **10+ units:** $65 each

Key Features:

- **Scannable Data:** QR codes link to embedded cardholder information such as name, photo, license number, and address.
- **Holograms:** Built-in reflective holographic patterns simulate real ID security elements.
- **UV Markings:** Hidden symbols or text visible under UV/black light.
- **Durability:** Made from Teslin, resistant to water, tearing, and chemical damage.
- **Relief Printing:** Raised text/numbers for tactile authenticity.
- **Laser Engraving:** Permanently etched data to prevent fading or tampering.

Customization Options:

Users can personalize all standard ID elements, including:

- Name, date of birth, license number, validity period
- Photo/avatar, signature, address
- Physical details (e.g., height, weight, eye color, gender)

Delivery Time

Orders are fulfilled and shipped within **12 days**.

Through direct engagement with the threat actor, CloudSEK Researchers successfully obtained a scannable sample of a counterfeit Georgia driver's license. The barcode was decoded, revealing detailed personal information of a real customer, including full name, address, date of birth, and driver's license number - confirming the card's functionality and potential for identity misuse.

Snapshot of the Scannable Barcode

Barcode: 1 of 1 Type: Pdf417
Length: 414 Rotation: none
Module: 2.0pix Rectangle: {X=315,Y=239,Width=571,Height=177}
Barcode Text processing:
Formatted: drvLic

Page 1 of 1

```
<AAMVA>
  <user>
    <last e="DCS"  [redacted] /last>
    <first e="DAC">Michael</first>
    <dob e="DBB"  [redacted] ob>
    <eyes e="DAY">BLK</eyes>
    <sex e="DBC">M</sex>
    <height e="DAU">5'7"</height>
    <weight e="DAW">158</weight>
    <street e="DAG"  [redacted] /street>
    <city e="DAI">Moultrie</city>
    <state e="DAJ">GA</state>
    <postal e="DAK"  [redacted] /postal>
    <country e="DCG">USA</country>
    <id e="DAQ">058138608</id>
    <issued e="DBD">2023-03-21</issued>
    <expires e="DBA">2031-01-10</expires>
  </user>
  <head>
    <filetype name="File Type">ANSI</filetype>
    <format name="Data Format">11</format>
    <issuer name="Issuer Identification Number">[redacted] /issuer>
    <state name="Issuer Name">Georgia</state>
    <st name="Issuer Name Abbreviated">GA</st>
    <version name="AAMVA Version Number">09</version>
    <jurver name="Jurisdiction Version Number">01</jurver>
    <entries name="Number of Entries">02</entries>
  </head>
  <subfile designator="DL" offset="41" length="250">
    <element id="DAQ" name="Customer ID Number"[redacted]
      </element>
    <element id="DCS" name="Customer Family Name"
      </element>
    <element id="DDE" name="Family name truncation">U</element>
    <element id="DAC" name="Driver First Name">MICHAEL</element>
    <element id="DDF" name="First name truncation">U</element>
    <element id="DAD" name="Driver Middle Name or Initial">
    </element>
    <element id="DDG" name="Middle name truncation">U</element>
    <element id="DCA" name="Jurisdiction-specific vehicle class"
>C</element>
```

Snapshot of the Barcode revealing the Driver License no, the buyer's full name along with other personal details

Through confidential sources, CloudSEK Researchers obtained a video demonstrating the verification of barcodes embedded on the back of the counterfeit driver's license cards. The scan was conducted using a device commonly employed at security checkpoints, building access gates, event entrances, and retail points-of-sale, confirming that these cards are fully scannable and emulate genuine licenses. This validates the threat actor's claims on their website and shows the potential for such IDs to bypass identity verification, age-restricted access controls, and other security screening processes. The proof-of-concept video showcasing this verification process can be accessed here.


```
    <element id="DBA" name="Document Expiration Date">
      </element>
    <element id="DBC" name="Physical Description - Sex">1
      </element>
    <element id="DAU" name="Physical Description - Height">067 i
n</element>
    <element id="DAY" name="Physical Description - Eye Color">BL
K</element>
    <element id="DAG" name="Address - Street 1">[redacted]
      </element>
    <element id="DAI" name="Address - City">MOULTRIE</element>
    <element id="DAJ" name="Address - Jurisdiction Code">GA
      </element>
    <element id="DAK" name="Address - Postal Code">
      </element>
    <element id="DCF" name="Document Discriminator">[redacted]
267023</element>
    <element id="DCG" name="Country Identification">USA</element
>
    <element id="DCK" name="Inventory control number"[redacted]
2</element>
    <element id="DDA" name="Compliance Type">N</element>
    <element id="DDB" name="Card Revision Date">01022019
      </element>
    <element id="DAW" name="Physical Description - Weight">158
      </element>
  </subfile>
  <subfile designator="ZG" offset="291" length="134">
    <element id="A" name="Optional field A">N</element>
    <element id="B" name="Optional field B">N</element>
    <element id="D" name="Optional field D">COLQUITT</element>
    <element id="E" name="Optional field E">N</element>
    <element id="F" name="Optional field F">[redacted]</element
>
    <element id="G" name="Optional field G">[redacted]
      </element>
    <element id="H" name="Optional field H">010</element>
    <element id="I" name="Optional field I">
      </element>
    <element id="J" name="Optional field J">MOULTRIE</element>
    <element id="K" name="Optional field K">GA</element>
    <element id="L" name="Optional field L">31768-0000</element>
    <element id="M" name="Optional field M">N</element>
  </subfile>
</AAMVA>
```


Snapshot of some other PII exposed within the scannable Barcode

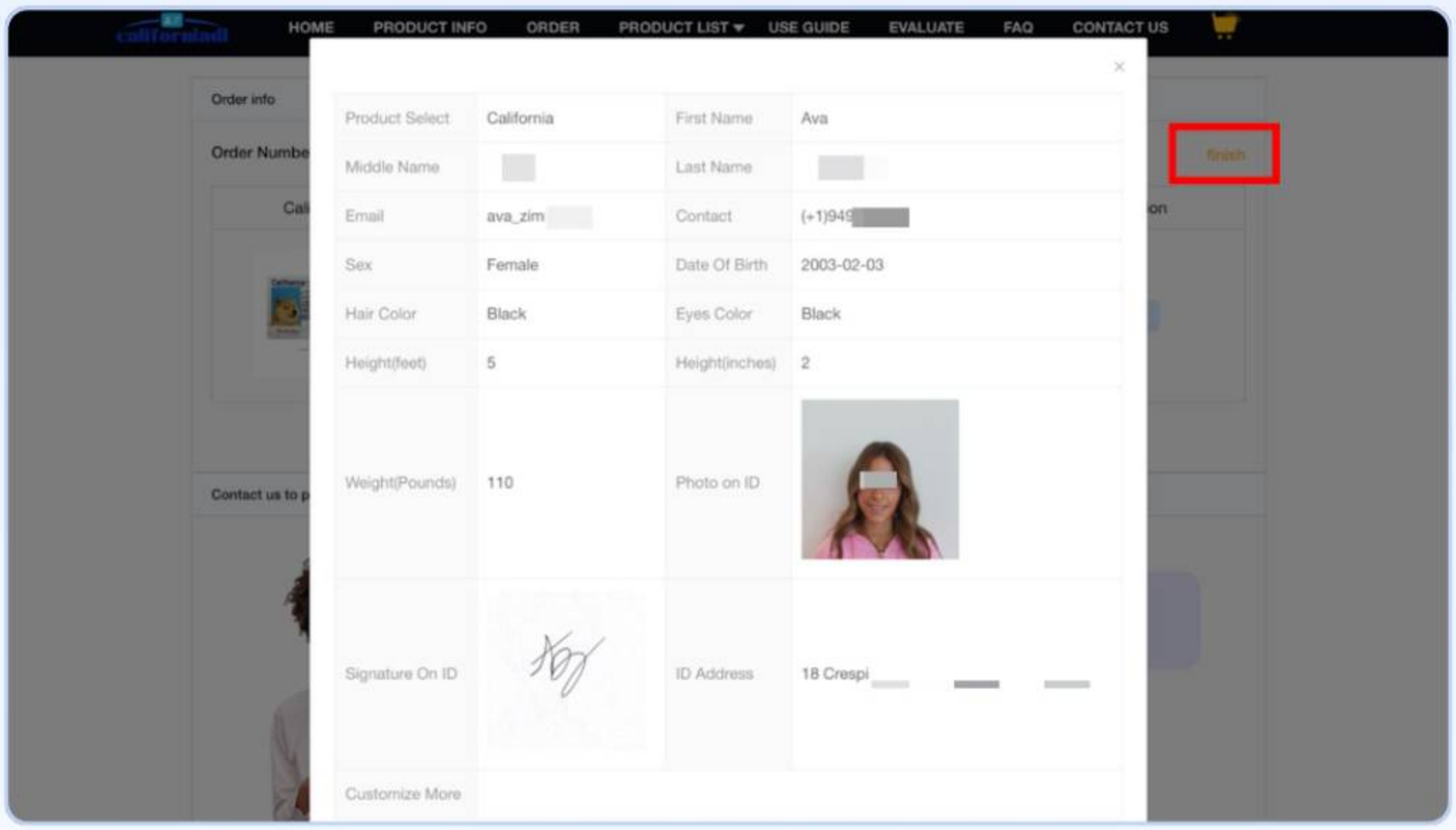
Snapshot of another redacted real sample of a counterfeit Georgia Driver License

Customer & Buyer Database

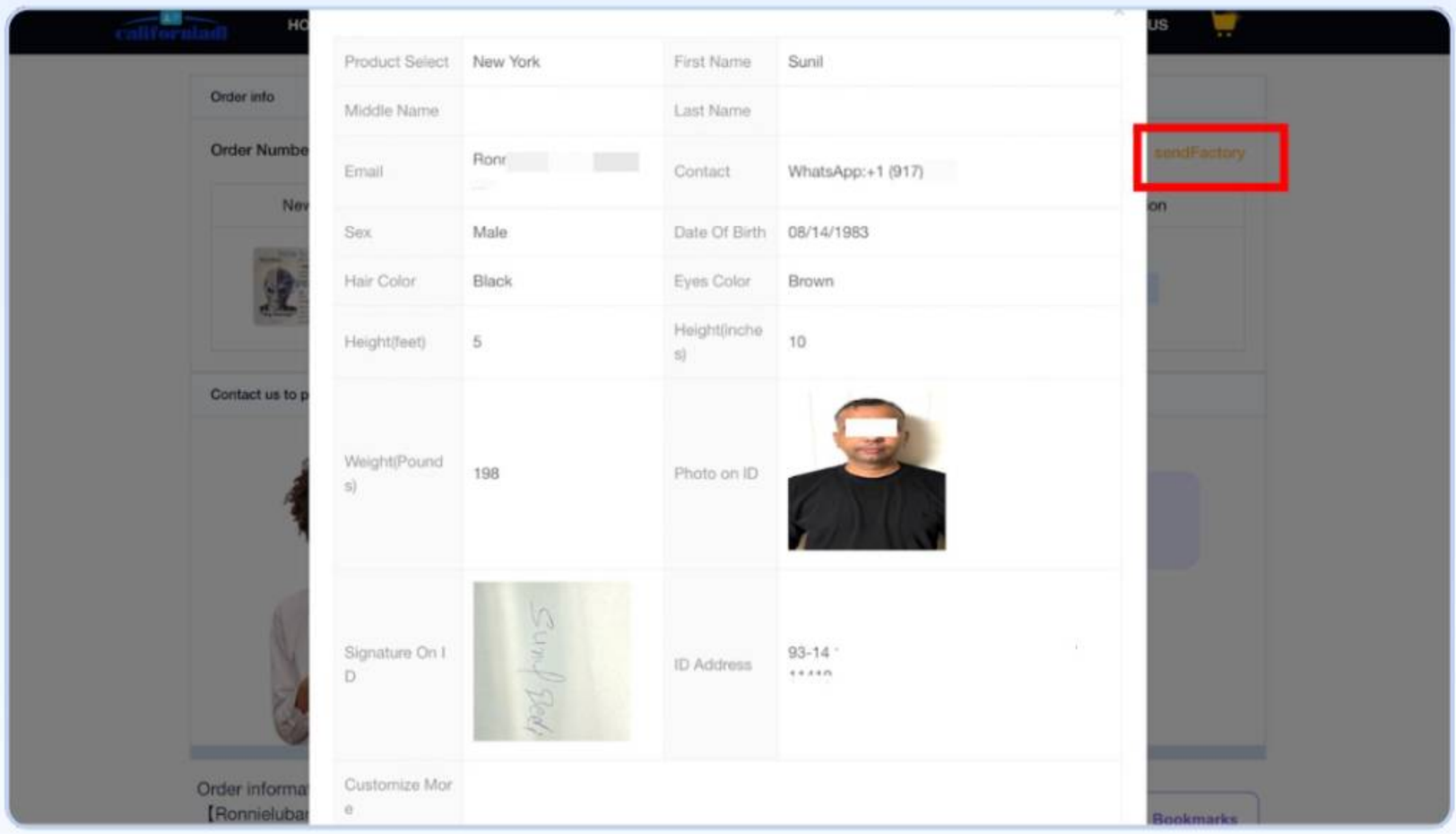
Researchers at CloudSEK identified a critical vulnerability within the threat actor's underlying infrastructure, which spans multiple interconnected websites used to distribute counterfeit identification documents. This weakness enabled the exfiltration of the full customer database - not limited to a single domain but encompassing all platforms operated under the same backend system.

The extracted data revealed personally identifiable information (PII) of **over 4,500 buyers** to date, with many buyers having purchased **multiple licenses for different names** and **individuals under the same Order ID**, bringing the **total number of counterfeit licenses sold** to over **6,500**. This PII includes:

- Full names and addresses
- Email addresses and mobile numbers
- IP addresses
- Uploaded images and signatures
- Payment methods, order history and much more
- Shell website to which the payment or checkout process redirects



*Snapshot of the vulnerability allowing the exfiltration of one of the buyer's PII data and their order status set as "**finish**"*



```
{
  "code":200,
  "timestamp":"2025-08-05 01:40:28",
  "message":"success!",
  "data":{
    "data":{
      "id":4889,
      "tradeNo":"",
      "orderNo":"28950",
      "coupon":"",
      "pay":"Apple Pay",
      "userId":"",
      "expressId":2,
      "express":50.00,
      "expedite":20.00,
      "handleFee":13.00,
      "totalFee":143.00,
      "submitIP":"174.  ",
      "createTime":"2025-08-02 09:1  :57",
      "payTime":"2025-08-02 09:38:52",
      "updateTime":"2025-08-05 01:23:50",
      "factoryTime":"2025-08-02 09:58:25",
      "cardTime":"2025-08-04 23:05:16",
      "expressTime":"",
      "sendTime":"",
      "cashTime":"2025-08-02 09:38:52",
      "updateUser":"",
      "remark":"更新跟进信息",
      "orderStatus":"createCard",
      "approvePhoto":"",
      "approveIP":"Chrome 13",
      "contact":"WB-旧:1229  ",
      "email":"smithm  ",
      "followStatus":1,
      "infoStatus":0,
      "infoRemark":"",
      "cashStatus":"arrived",
      "cashUser":"富强",
      "cashFee":"$ 136.41",
      "payPath":"",
      "payName":"",
      "userName":"",
```

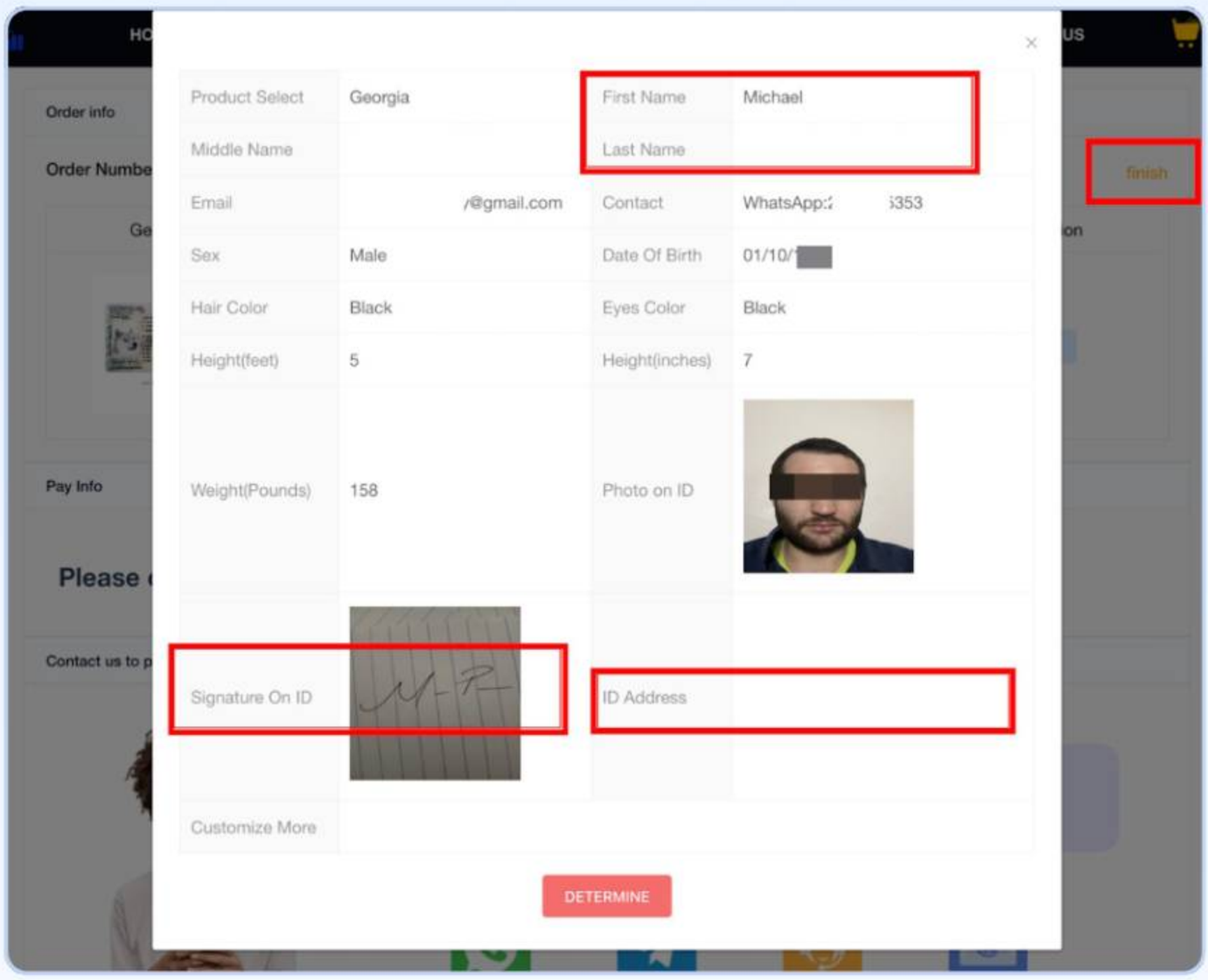

Snapshot of the JSON response body revealing buyer's details


```
    "place":{
      "id":4877,
      "memberId":"",
      "orderId":4889,
      "address":"3962  ",
      "receiver":"John  ",
      "country":"",
      "state":"",
      "city":"",
      "mobile":"229  "
    },
    "list":[
      {
        "id":10934,
        "proType":1,
        "memberId":"",
        "orderId":4889,
        "productId":829,
        "count":1,
        "price":90,
        "totalFee":0,
        "payFee":90,
        "orderStatus":"createCard",
        "createTime":"2025-08-02 09:16:57",
        "contactEmail":"smith  ",
        "contact":"WhatsApp:4  ",
        "state":"Utah",
        "firstName":"Zachary",
        "middleName":"",
        "lastName":"  ",
        "birthday":"03/15/1983",
        "heightFeet":5.0,
        "heightInches":7.0,
        "weight":160.0,
        "eyesColor":"Black",
        "hairColor":"Black",
        "gender":"Male",
        "idAddress":"652 E  ",
        "idPhotoPath":
        "/phdcard/profile/  ",
        "attach":"",
```


Snapshot of the JSON response body revealing buyer's details

Further analysis of the exfiltrated buyer database confirmed the presence of the same individual (ie **Michael** *****) whose counterfeit Georgia driver's license was obtained as a sample via direct engagement with the threat actor (as stated in the previous section). Key personal details - such as full name, date of birth, height, weight, and other identifiers - **exactly matched** the information extracted from the scannable barcode on the license.

Additionally, the database entry showed the buyer's **payment status as "finish"**, indicating a **successful transaction and confirmed delivery**. This correlation strongly reinforces the credibility of the operation and proves that the counterfeit licenses - complete with all advertised features - are indeed being actively produced and delivered by the threat actors.



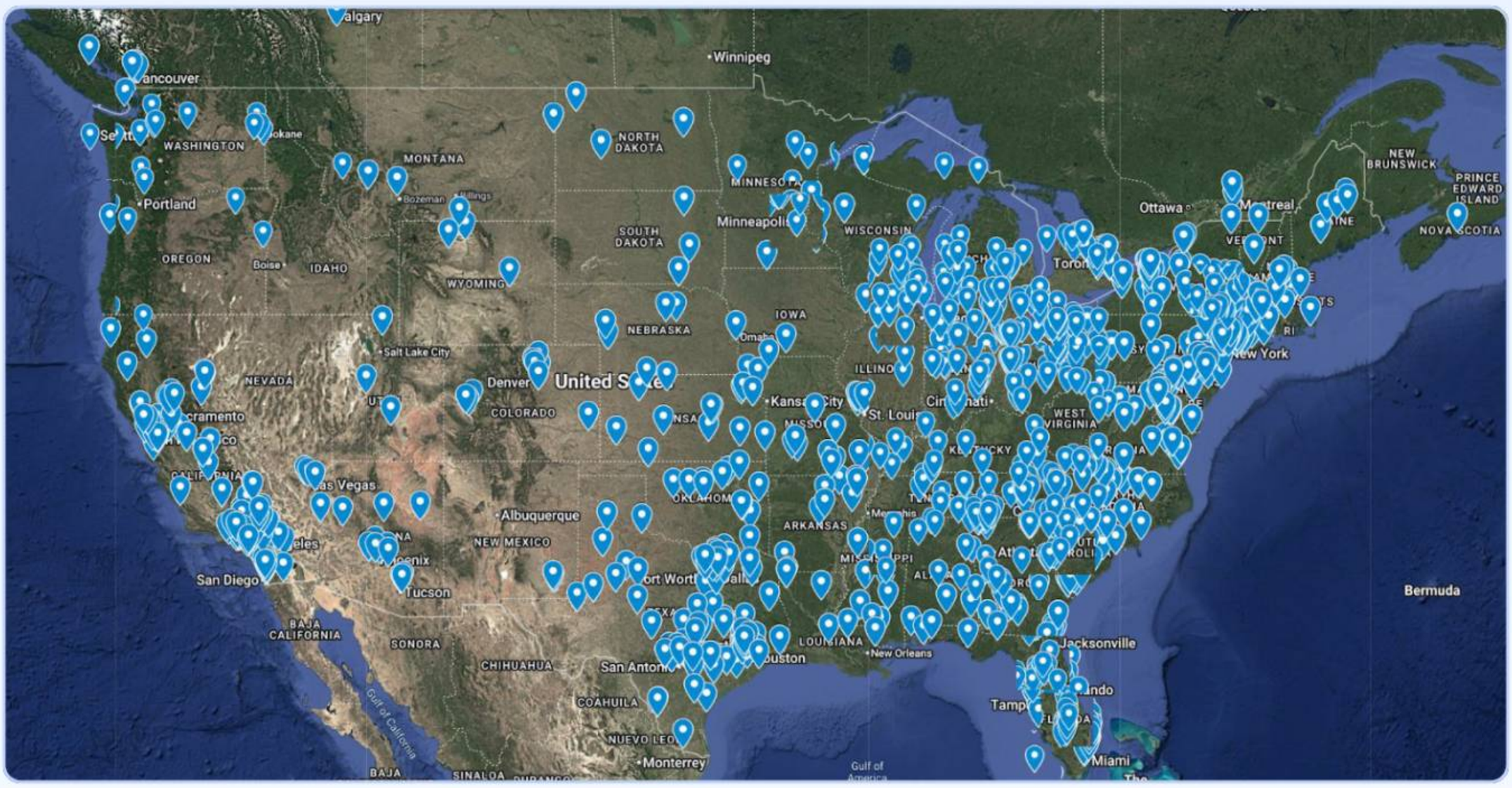
*Snapshot of the buyer/customer, Michael *****'s data records aligning exactly with the sample driver license card obtained along with the PII, signature, image, etc. and order status set as "**finish**" indicating that this was a valid purchase and the payment was successfully done*

The earliest Order ID in the database, created by the threat actor for testing purposes, dates back to **2023**, indicating that this campaign has been active for **at least two years** under the same maintained infrastructure.

Geospatial Distribution of Buyers

Using the exfiltrated buyer/customer database, researchers at CloudSEK geolocated mailing addresses and plotted them as pinpoints on a satellite-based geospatial map. The plotted distribution reveals a **heavy concentration of buyers within the United States**, with the highest densities along the **Eastern Seaboard** and notable clusters in **New York, Pennsylvania, Florida, and Georgia**, as well as **Texas, California, and Illinois**.

Beyond the U.S., smaller but distinct clusters of buyers appear in **Canada**, particularly in the provinces of **Ontario, British Columbia, and Alberta**.



Snapshot displaying the payment methods once a buyer fills up the order form

Financial Footprinting

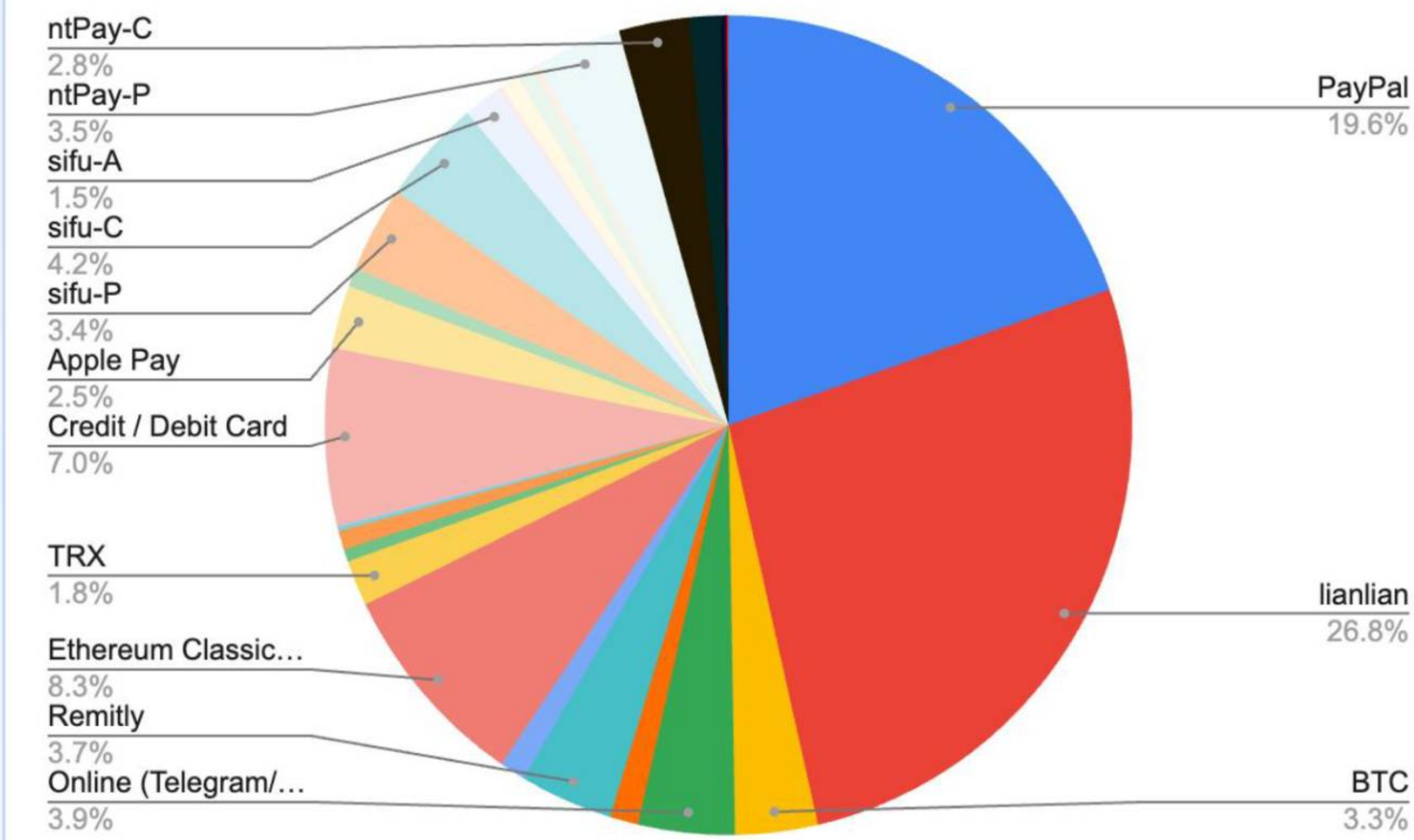
Through analysis of the exfiltrated buyer and customer database, CloudSEK Researchers were able to estimate the **total revenue generated** by the threat actor group based on the payment records of counterfeit document purchases. The cumulative earnings from all recorded transactions amounted to **over $785,000 USD**, underscoring the **significant financial scale** of the operation.

The dataset also revealed the **diverse range of payment methods** used by buyers, including:

- PayPal, LianLian, PayBitcoin (BTC), Ethereum Classic(ETC), Apple Pay, Credit/Debit Cards, NT Payments, Remitly, etc.

These insights not only highlight the global accessibility of the operation but also point to deliberate efforts by the operators to offer **multiple payment channels** to accommodate buyers across different regions.

A pie chart illustrating the distribution of payment methods is shown below.



__LianLian Pay__ leads as the most commonly used payment method at __26%__, followed by __PayPal__ at __19.6%__. Together, these two platforms account for nearly half of all recorded transactions, highlighting user preference for accessible and semi-anonymous digital payment options

Cryptocurrency Tracking

From multiple websites operated under the same infrastructure, CloudSEK Researchers identified **four Cryptocurrency wallet addresses** linked to the threat actors. These are as follows:

- bc1pnyyqck89ycxjhpqa4r8dgcy5jfy96l78ekzklh9jvv6nh30frwuqwaa546
- 17WBMQNzx6pRuTqTa5cPRb3qRkgm42SBQ3

- TTKBZgkRgfbthJdpB9ukTk9×11LzBWQHKo
- 0×11b65a7b4765957ace98da24B0BD9E3C13D4dEA5

One particular Bitcoin (BTC) Wallet Address showed the following activity:

- **82 total transactions**
- **Received:** 0.18563481 BTC (**~$21,397.47**)
- **Sent:** 0.16335481 BTC (**~$18,829.34**)
- **Current balance:** 0.02228000 BTC (**~$2,568.14**)

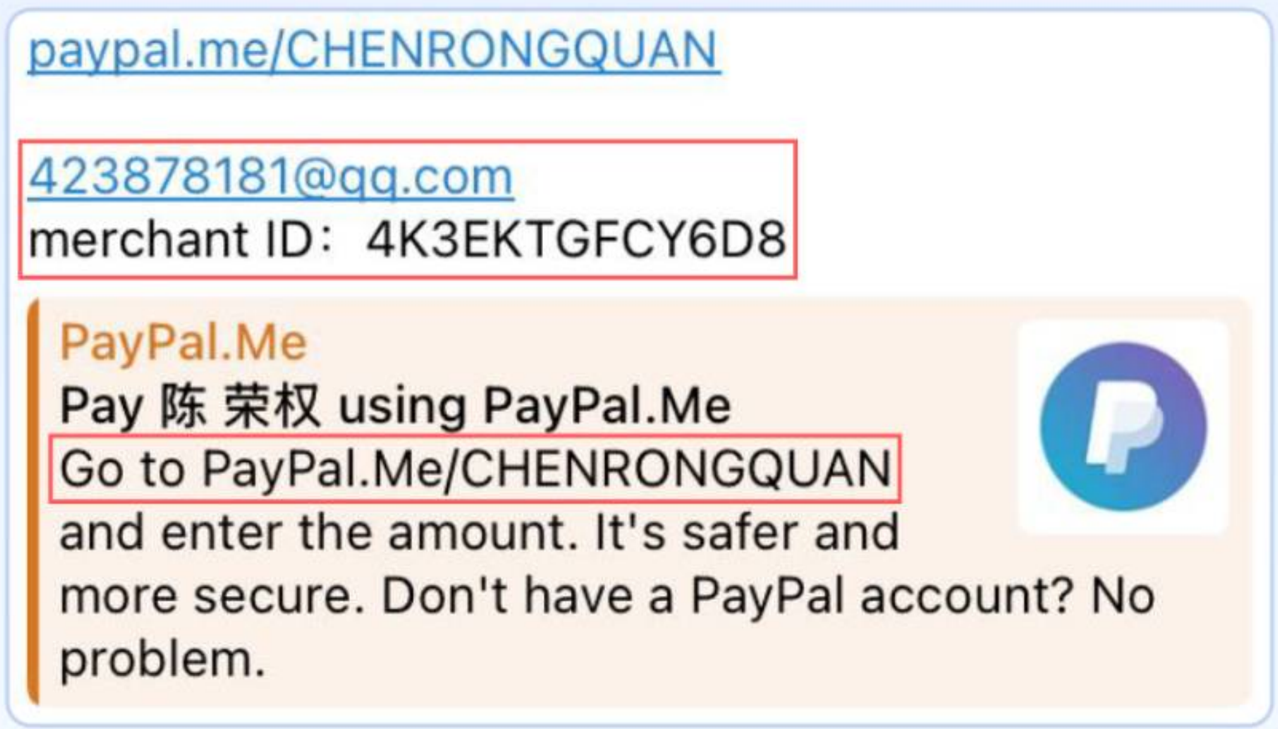
The amount received by this wallet **($21K+)** alone accounts for approximately **3% of the total revenue ($785K+)**, aligning closely with the **BTC transaction share** shown in the pie chart derived from the buyer database. These findings further validate the financial activity observed through both infrastructure analysis and database exfiltration.

Merchant Accounts

Through HUMINT engagement with the threat actor, CloudSEK Researchers identified a **PayPal account** and a **Western Union bank account** potentially used to **receive payments via direct communication channels**, separate from the standard checkout flow on the websites. These may represent **alternative payment methods** offered to certain buyers likely having issues with the regular checkout and payment process offered by the threat actor's websites.

Such transactions are potentially reflected as **"online" payments** in the exfiltrated backend database and differ from those processed through the default payment infrastructure.

Following these direct payments, the associated Order IDs, order statuses, and total payment values were potentially logged within the backend systems - suggesting a linkage between these off-platform transactions and the threat actor's broader infrastructure.



Snapshot of the PayPal Merchant Account reflecting the Threat Actor's Potential Full Name and the email address used by the QQ Mail Service provider

You can use Western Union to transfer money online.
The century-old brand is trustworthy.
The specific steps are as follows:
1. Click this link to log in to your Western Union account
https://partners.westernunion.com/us/en/web/send-money/start
2. Fill in transfer information
2.1 Select receiver's country: China
2.2 Send amount: 176 USD
2.3 How does your receiver want the money?
● Select: Mobile wallet
● Select: WeChat
2.4 Receiver's first name: RONGQUAN
2.5 Receiver's last name: CHEN
2.6 Wallet ID: 15605928959
2.7 Purpose of transaction: Purchase of Goods
3. Payment successful
Please provide a screenshot of the transfer.
Thank you! 🙏

Snapshot of the Threat Actor's potential Personal Bank Account reflecting the same name linking this Western Union Bank Account back to them and the receiver's county as ***China***

Threat Actor Attribution

CloudSEK researchers were also successfully able to attribute the threat actor behind the entire operation. Through a combination of HUMINT and OSINT, the team extracted precise geolocation data, pinpointing the threat actor's exact coordinates in **Huli District, Xiamen, Fujian, China**.

Additionally an operational security lapse on one of the threat actor's infrastructure sites revealed a matching address.

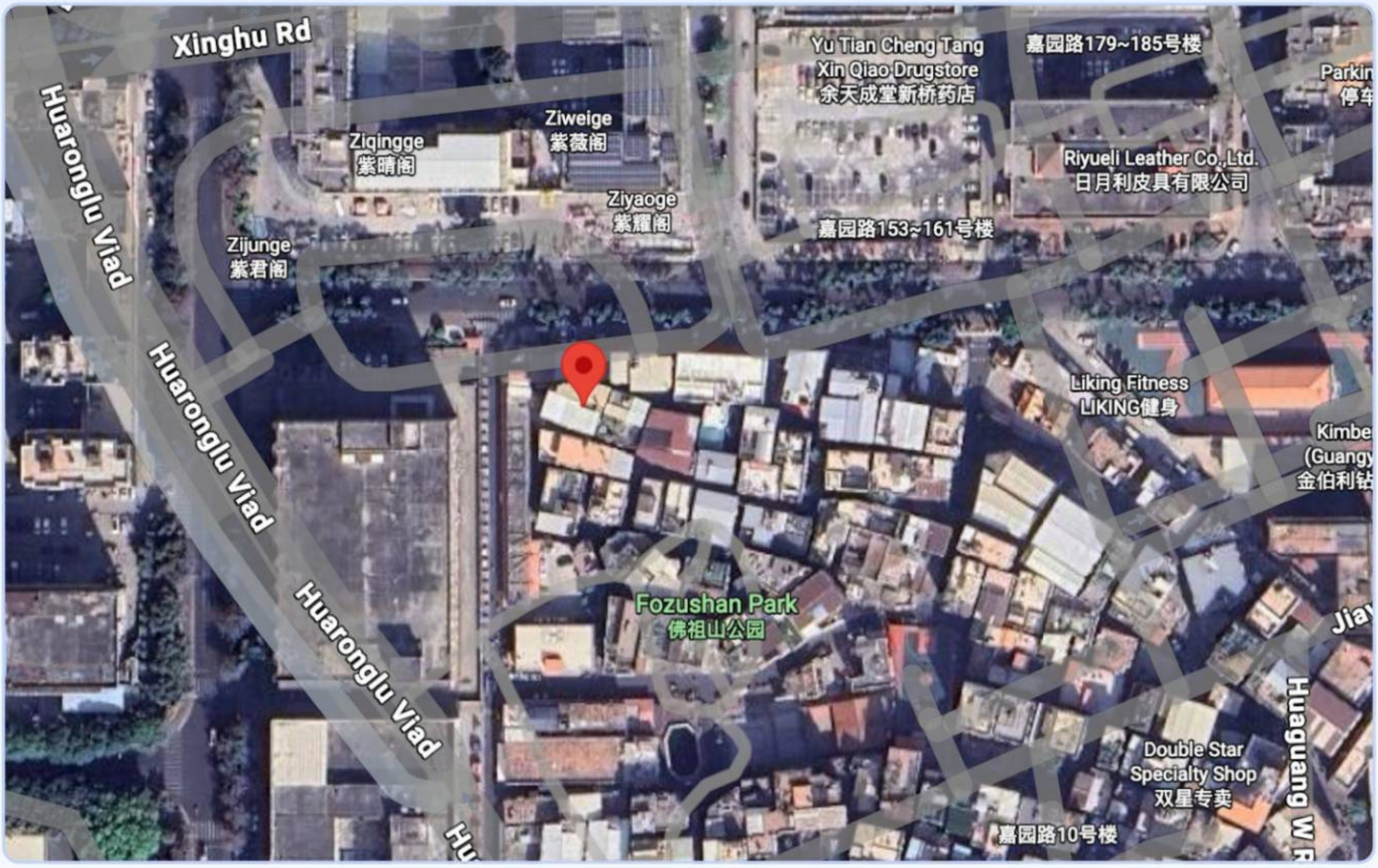
Email: idcacas@proton.me

Phone: +86 132 9876 5432

Address: Xiamen, Fujian, China

© 2025 Xiamen IDCACA. All rights reserved.

Snapshot of a matching address revealed in one of the domains owned by the Threat Actor



Snapshot of the Threat Actor's exact geolocation on [Google Maps]

Further engagement with the threat actor made it possible for CloudSEK researchers to also obtain a **facial image** of the individual through their **webcam**. This was achieved via a controlled engagement environment that prompted the actor to unintentionally reveal their webcam feed.

Snapshot of the Threat Actor's facial image obtained through their webcam

The combination of **precise geolocation data** and **visual identification** significantly enabled a robust, high-confidence attribution of the threat actor behind the large-scale fraudulent operation.

However, considering the various operational facets such as production, packaging, and customer support, it is likely that more individuals are involved along with the identified threat actor.

Product Packaging and Delivery

Analysis of the threat actor's infrastructure revealed detailed information regarding the packaging and delivery process offered to buyers. Based on the available data, the threat actor provides **global delivery** and a buyer can typically expect to receive a **customized fake ID card within approximately 12 days**, under the fastest production and shipping conditions.

Card Production Timeline :

- **Standard Production:** 4 - 5 days | Free of charge
- **Expedited Production:** 2 - 3 days | $20 for 1 - 2 cards, +$10 for each additional card

Shipping Options :

- **Standard Shipping:** 10 - 14 days | $20
- **Express Shipping:** 6 - 8 days | $50

Delivery & Tracking Options :

- After production, a digital copy of the ID is sent to the buyer for confirmation.
- 2 - 3 days after shipping, tracking information is shared to monitor the delivery.

Courier Companies Used :

- FedEx
- USPS
- Gofo
- DHL
- Canada Post
- eMile

Covert Packaging Techniques

Undisclosed sources revealed **sophisticated concealment methods** used to ship fake licenses in a manner designed to evade customs and law enforcement detection.

- The fake ID cards are shipped inside **a regular cardboard box**, which, when opened, appears to contain **ordinary items** such as a purse, toy, or other harmless consumer goods.

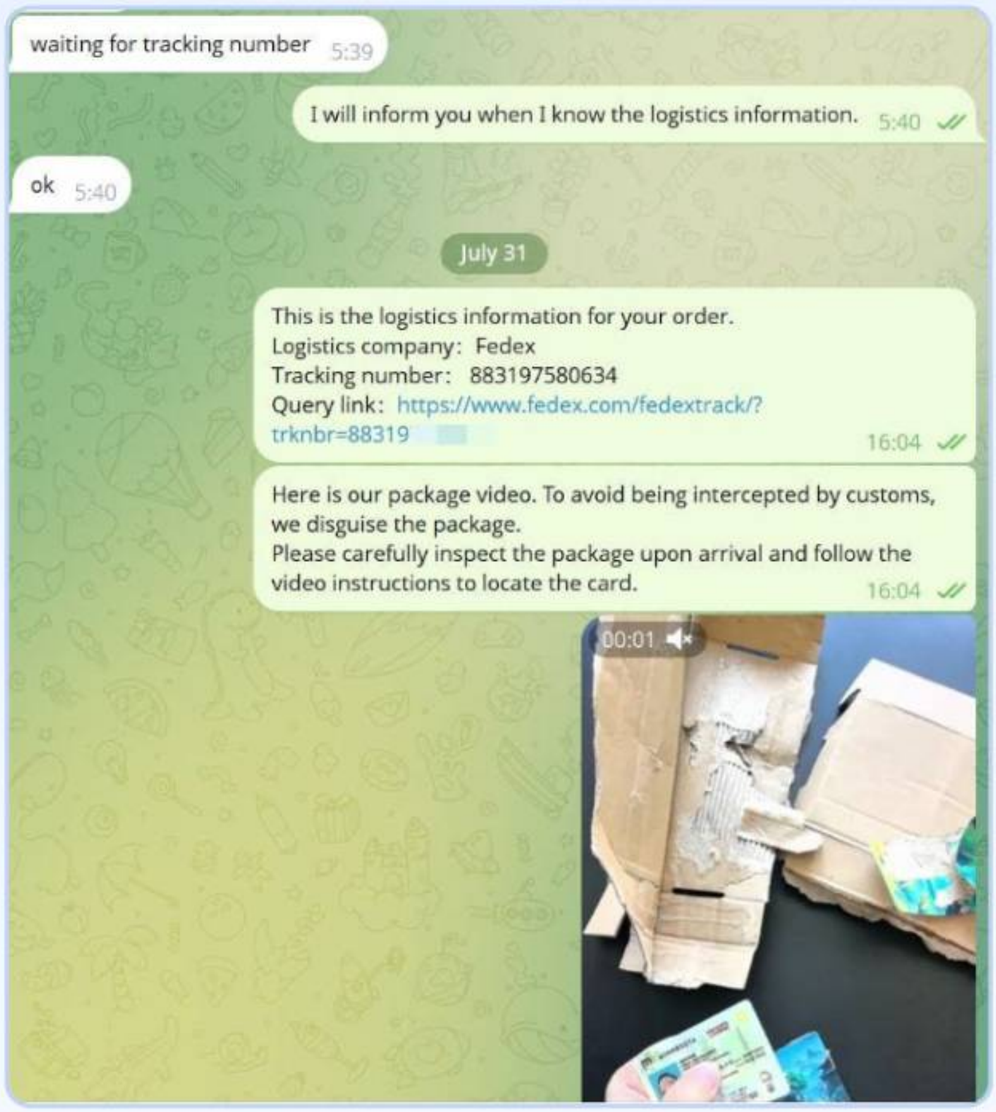
- However, when the **cardboard is torn open from the middle**, the buyer discovers the **hidden ID cards** embedded inside the layers of the box.

To further reduce the chances of detection:

- Each card is covered with a **plastic film sticker**, which serves as a **camouflage layer**, making the card look like a harmless item.
- Once this **protective sticker is peeled off**, the fake ID becomes fully visible and usable.

Delivery Verification

As part of the investigation, CloudSEK researchers were able to obtain a conversation between the threat actor and a buyer, which revealed a **FedEx tracking ID** linked to a completed shipment.



Snapshot of logistics information sent by the threat actor to a customer

- The tracking ID, when analyzed, showed a parcel sent from **Yiwu, China** to **Caledon, Canada**.

Wednesday, 7/30/25	10:51 PM	Shipment information sent to FedEx	
Thursday, 7/31/25	1:58 PM	Picked up	YIWU CN
	4:13 PM	Left FedEx origin facility	YIWU CN
	11:19 PM	International shipment release - Export	SHANGHAI CN
	11:26 PM	On the way	SHANGHAI CN
Friday, 8/1/25	12:49 AM	Arrived at FedEx hub	MEMPHIS, TN
	4:01 AM	On the way	MEMPHIS, TN
	4:16 AM	Departed FedEx hub	MEMPHIS, TN
	7:06 AM	At destination sort facility	MISSISSAUGA, ON
	7:28 AM	International shipment release - Import	MISSISSAUGA, ON
	9:46 AM	At local FedEx facility	WOODBRIDGE, ON
	9:56 AM	On FedEx vehicle for delivery	WOODBRIDGE, ON
	3:14 PM	Delivered	CALEDON, ON

Snapshot displaying the travel history of the shipment

Shipment facts

Shipment overview

TRACKING NUMBER	8831 [redacted]
DELIVERED TO	Residence
SHIP DATE	7/31/25
STANDARD TRANSIT	8/1/25 before 5:00 PM
DELIVERED	8/1/25 at 3:14 PM

Services

SERVICE	FedEx International Priority
TERMS	Shipper
SPECIAL HANDLING SECTION	Deliver Weekday, Residential Delivery

Package details

WEIGHT	0.44 lbs / 0.2 kgs
DIMENSIONS	12x11x1 in.
TOTAL PIECES	1
TOTAL SHIPMENT WEIGHT	0.44 lbs / 0.2 kgs
PACKAGING	FedEx Pak

Snapshot displaying the shipment facts of the product

- The tracking data confirmed that the package was **successfully delivered**, with the package being **left at the recipient's front door**.

Snapshot displaying the package left at the buyer's front door

Additionally through undisclosed sources, we identified another shipment tracking ID, which led us to a **photograph of the packaged shipment**.

The label displayed the recipient's name as **Param Ja****** with the address **13859 Oak Leaf Way, Ra**** Cu*******, CA 91*****.

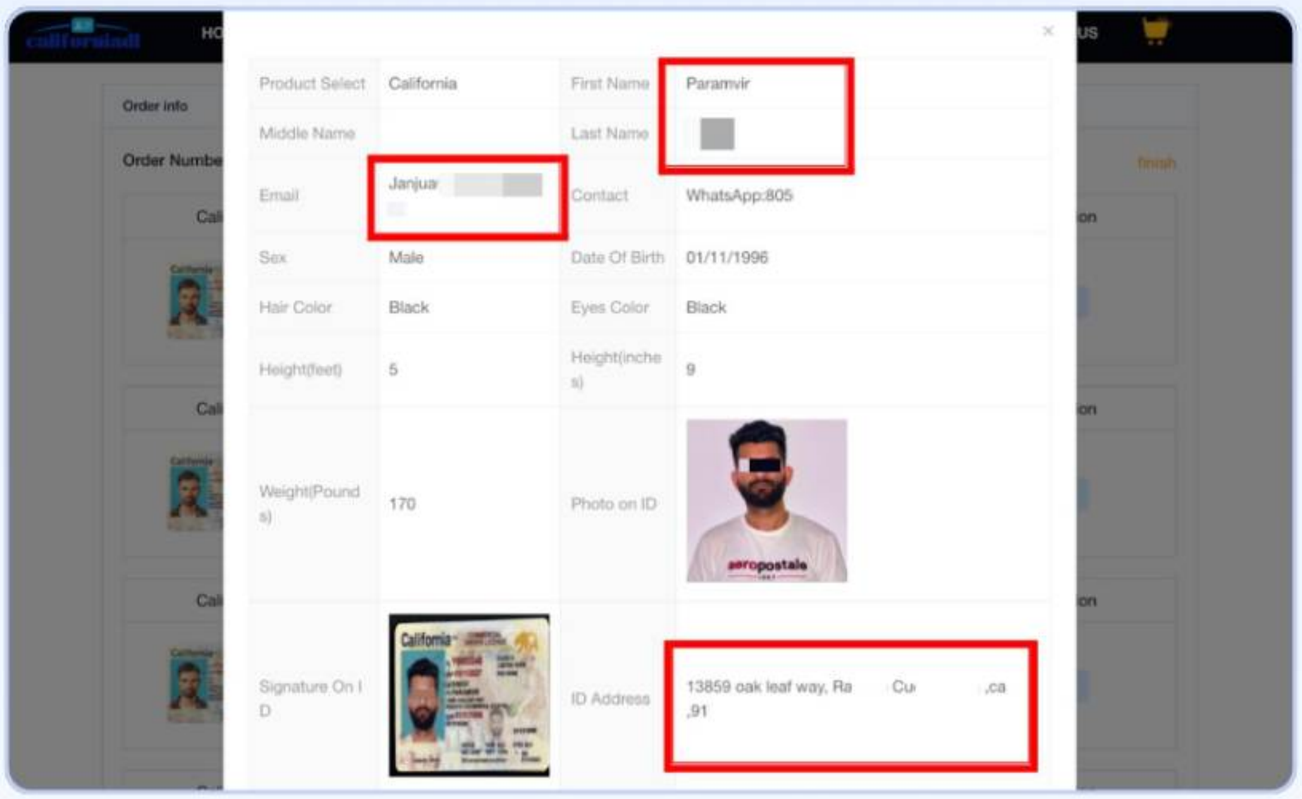
This information exactly matched the receiver's details in our extracted customer database. We also observed that the individual had placed the order requesting the name on the license to be **Paramvir S****.

*Snapshot of the package with receiver's name as Param J***** and address as 13859 Oak Leaf Way, R***** C*******, CA 91****


```
"place":{
  "id":2824,
  "memberId":"",
  "orderId":2828,
  "postCode":"",
  "address":"13859 oak leaf way,Ra     Cu     ,Ca,91",
  "receiver":"Param Ja ",
  "country":"",
  "state":"",
  "city":"",
```


Snapshot displaying matching receiver's name and address extracted from the customer database

This discovery not only validates the threat actor's ability to fulfill international orders but also highlights the use of **legitimate courier services** to deliver fake identification documents while maintaining a facade of normalcy.



*Snapshot displaying the order made by the buyer with the order status as **finish***

Additionally, buyers are provided with a **tutorial video** that guides them step-by-step on how to locate and retrieve the hidden cards. We were able to obtain a copy of this video, which can be viewed here.

By analyzing the fake license card shown in the tutorial and cross-referencing it with records from the exfiltrated customer database, researchers found another exact match - further confirming the authenticity of the license distribution network.

Snapshot displaying the ID card from the tutorial video matching with the buyer details

Product Select	Minnesota	First Name	[redacted]
Middle Name	ABDU[redacted]	Last Name	IBRAHIM
Email	Mohameda[redacted]	Contact	WhatsApp:17632[redacted]
Sex	Male	Date Of Birth	02/27/2000
Hair Color	Black	Eyes Color	Black
Height(feet)	6	Height(inches)	1
Weight(Pounds)	160	Photo on ID	
Signature On ID		ID Address	15460 EAMES [redacted]
Customize More	ISS 05/07/2024 EXP 02/27/2028 DL# N014-12[redacted] CLASS D		

*Snapshot displaying the order made by the buyer with the order status as **finish***

Case Study: Obtained Fake Driver's Licenses Potentially Linked to Large-Scale Illegal Operations

As mentioned in the previous section, we identified a confirmed shipment to **Param J******* (also known as **Paramvir S*****). During our investigation, we uncovered two suspicious orders placed by the same individual. These orders accounted for **42 fraudulent commercial driver's licenses** purchased for **USD 2,190**, each containing different names, photographs, and license numbers. Tracing these orders further, we found they were all linked to a single email address, which became a key pivot point in our analysis.

Through basic open-source intelligence (OSINT), we found that this email address was also associated with two trucking and transportation businesses: **Janjua Transport** (MC1236841, USDOT 3620976) and **AP Freight Trucklines Inc.** (USDOT 3932312, MC1457821). Notably, the same individual's name appeared both in our customer database and in the company registration details.

Further digging into official Federal Motor Carrier Safety Administration(FMCSA) records revealed compliance issues with both entities. In 2022, Janjua Transport's operating authority was **revoked** following regulatory action. Similarly, AP Freight Trucklines Inc.'s authority was **revoked**, though the company later submitted evidence of compliance and had its certificate **reactivated**. These official enforcement records underscore the history of non-compliance tied to entities connected with the same email used to purchase fake drivers licenses.

BrokerSnapshot
https://brokersnapshot.com › Company

JANJUA TRANSPORT

Contacts · ANNIE STEPHANIE GOMEZ DELGADO · (805) 635-4262 · (661) 865-1817 · janj[redacted]@gmail.com · PARAMVIR [redacted]

BrokerSnapshot
https://brokersnapshot.com › Company

AP FREIGHT TRUCKLINES INC

(805) 792-2657 8/10/2022. janj [redacted]@gmail.com 8/10/2022. PARAMVIR [redacted] 8/10/2022. General. 2022. 10 changes. 8/9/2022 · 8/10/2022 · 8/15/2022 · 9/9/2022 · 9/14 ...

*Note: **The USDOT number** is a unique identifier issued by the Federal Motor Carrier Safety Administration to track a company's safety and compliance record. **The MC number** (Motor Carrier number) grants a company the legal authority to operate as a for-hire carrier or broker across state lines.*

MC-1236613-C	SNOW WHITE TOURS AND TRAVEL LLC - ROCHESTER, NY	06/14/2022	REVOCATION
MC-1236840-C	METHODICAL TRUCKING LOGISTICS LLC - NASHVILLE, TN	06/14/2022	NOTICE
MC-1236841-C	JANJUA TRANSPORT - BAKERSFIELD, CA	06/14/2022	REVOCATION
MC-1236865-C	EDSON FERNANDO MANSILLA ROJAS AND EMILY J - HOUSTON, TX	06/14/2022	NOTICE
MC-1236965-C	ROAD READY CARGO LLC - ALPHARETTA, GA	06/14/2022	DISCONTINUANCE

Snapshot from FMCSA's official document

U.S. Department of Transportation
Federal Motor Carrier Safety Administration

1200 New Jersey Ave., S.E.
Washington, DC 20590

SERVICE DATE
February 28, 2023

DECISION

MC-1457821-C
AP FREIGHT TRUCKLINES INC
BAKERSFIELD, CA

REINSTATEMENT OF AUTHORITY

On December 27, 2022, AP FREIGHT TRUCKLINES INC, was notified that its certificate was revoked by the Federal Motor Carrier Safety Administration.

AP FREIGHT TRUCKLINES INC, has now filed a written request for reinstatement of the authority and has submitted evidence of compliance with 49 U.S.C § 13906 and 49 CFR 387.

It is ordered:

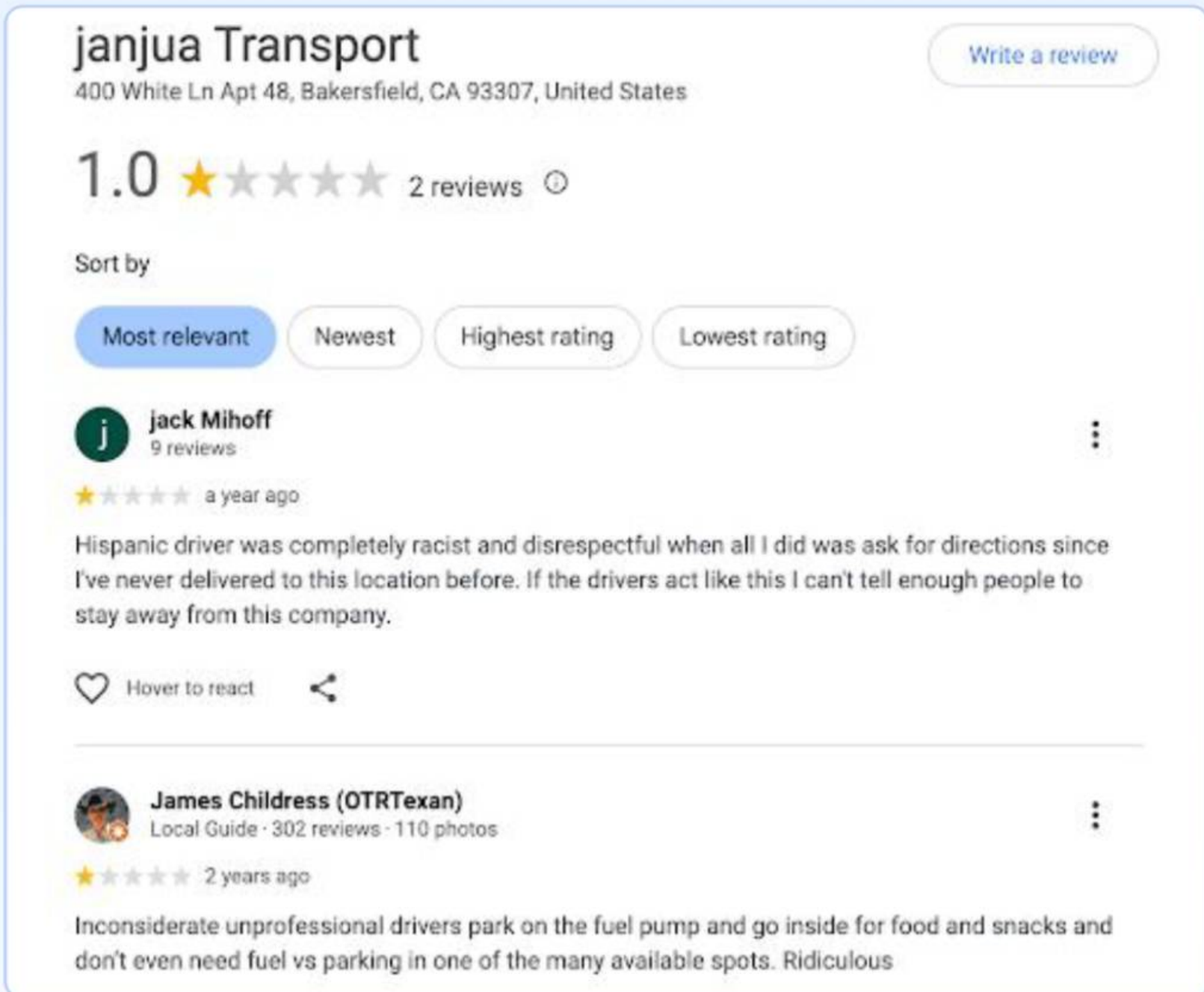
The certificate evidenced in Docket No. MC-1457821-C is reactivated. The effective date of the reinstatement of this authority is shown below.

Decided: February 28, 2023
By the Federal Motor Carrier Safety Administration

Jeffrey L. Secrist, Division Chief
Office of Registration

Snapshot from FMCSA's official document

In addition, a review of Janjua Transport's Google business profile revealed **customer complaints regarding driver behavior.** When considered together, these findings raise significant red flags. The fraudulent driver's licenses could be used to bypass KYC checks, skirt compliance requirements, enable unauthorized drivers to operate heavy vehicles, or even facilitate illicit activities such as smuggling, trafficking or fraudulent logistics operations.

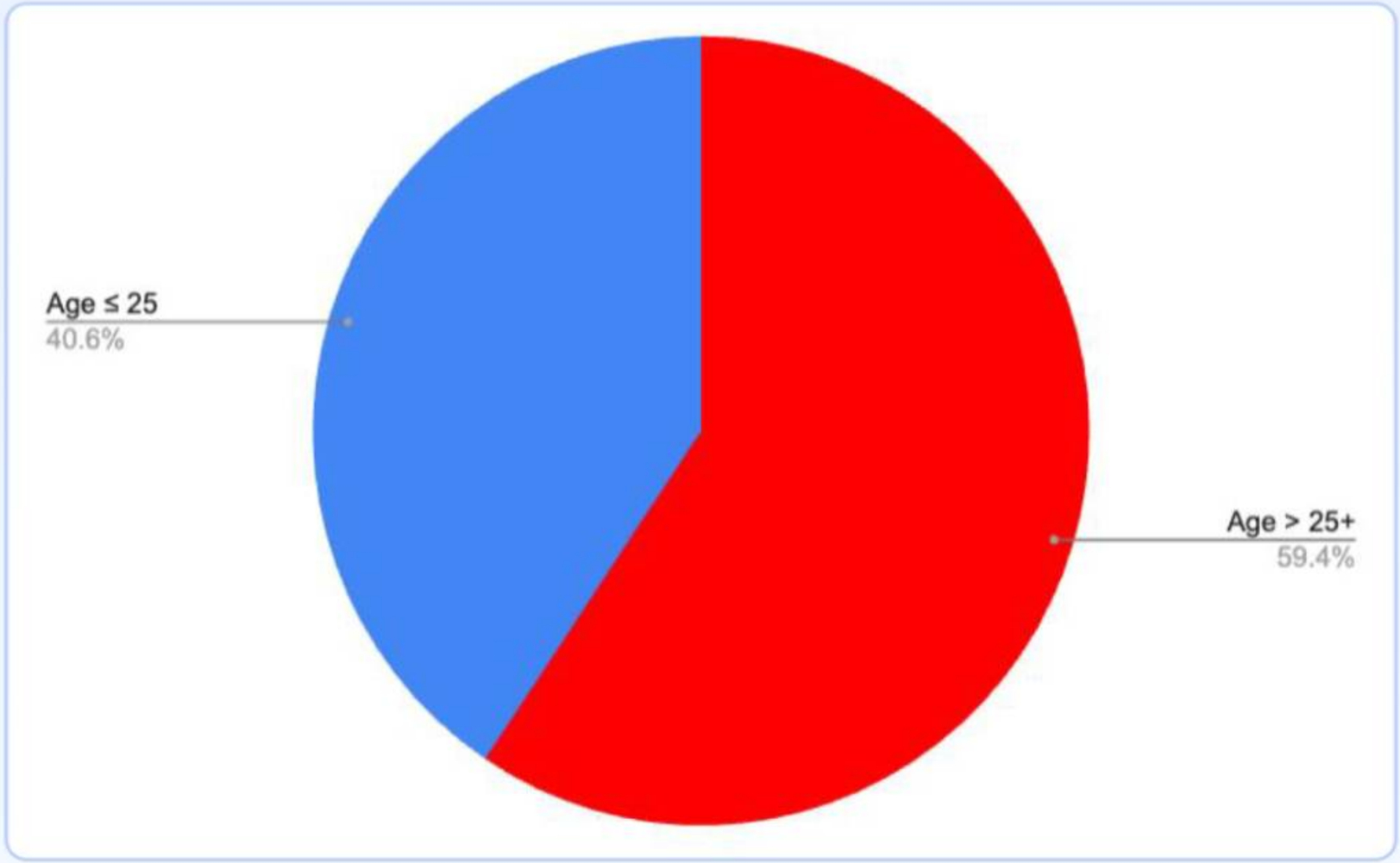


Snapshot of the Google review for Janjua Transport

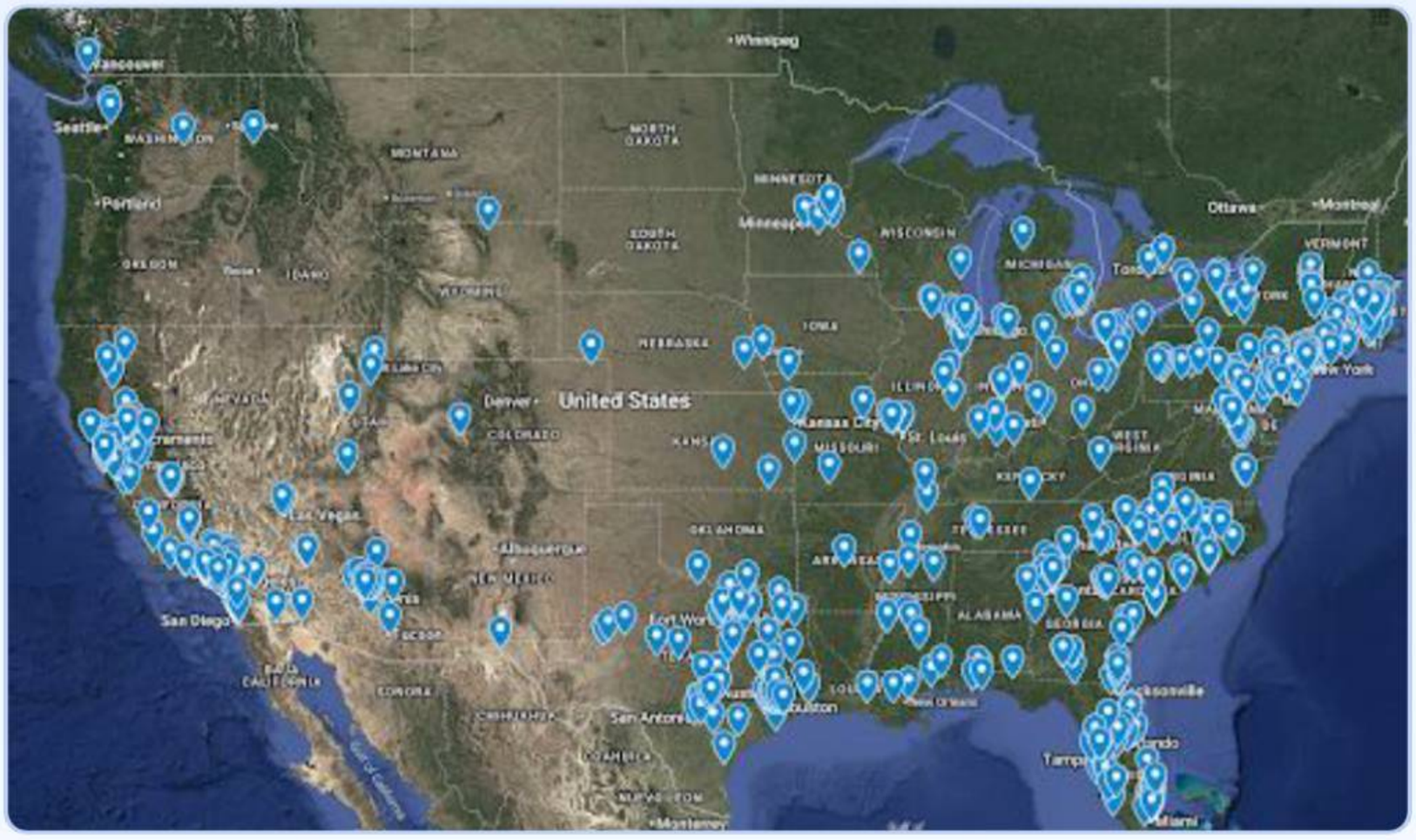
This case study demonstrates that the fake ID marketplace under review is not simply catering to individuals seeking personal misuse. Instead, it highlights how such services can be leveraged in ways that threaten **transportation security, regulatory integrity, and potentially national security itself**.

Additionally from the dataset of over **6,500 fraudulent driver's licenses**, we observed that approximately **2,640 IDs listed ages of 25 or below**. This suggests that a portion may have been obtained by underage individuals, potentially to bypass age restrictions for activities such as accessing adult material or restricted venues.

However, the larger and more concerning share about **3,860 IDs listed ages above 25**. When compared with the associated photographs, many of these ages appeared consistent with the individuals, raising the possibility that these documents are being used to facilitate **serious crimes with broader national security implications**. Importantly, while the IDs tied to minors may seem less threatening, they should not be dismissed, as they still present opportunities for criminal misuse.



Pie chart showing that 40.6% of the fake driver's licenses list ages below 25, while the majority 59.4% are for individuals aged 25 above, raising serious concerns that these documents may be exploited by adults to facilitate serious criminal activity



Geospatial distribution of customers/buyers potentially above the age of 25

Propagation & Marketing Techniques

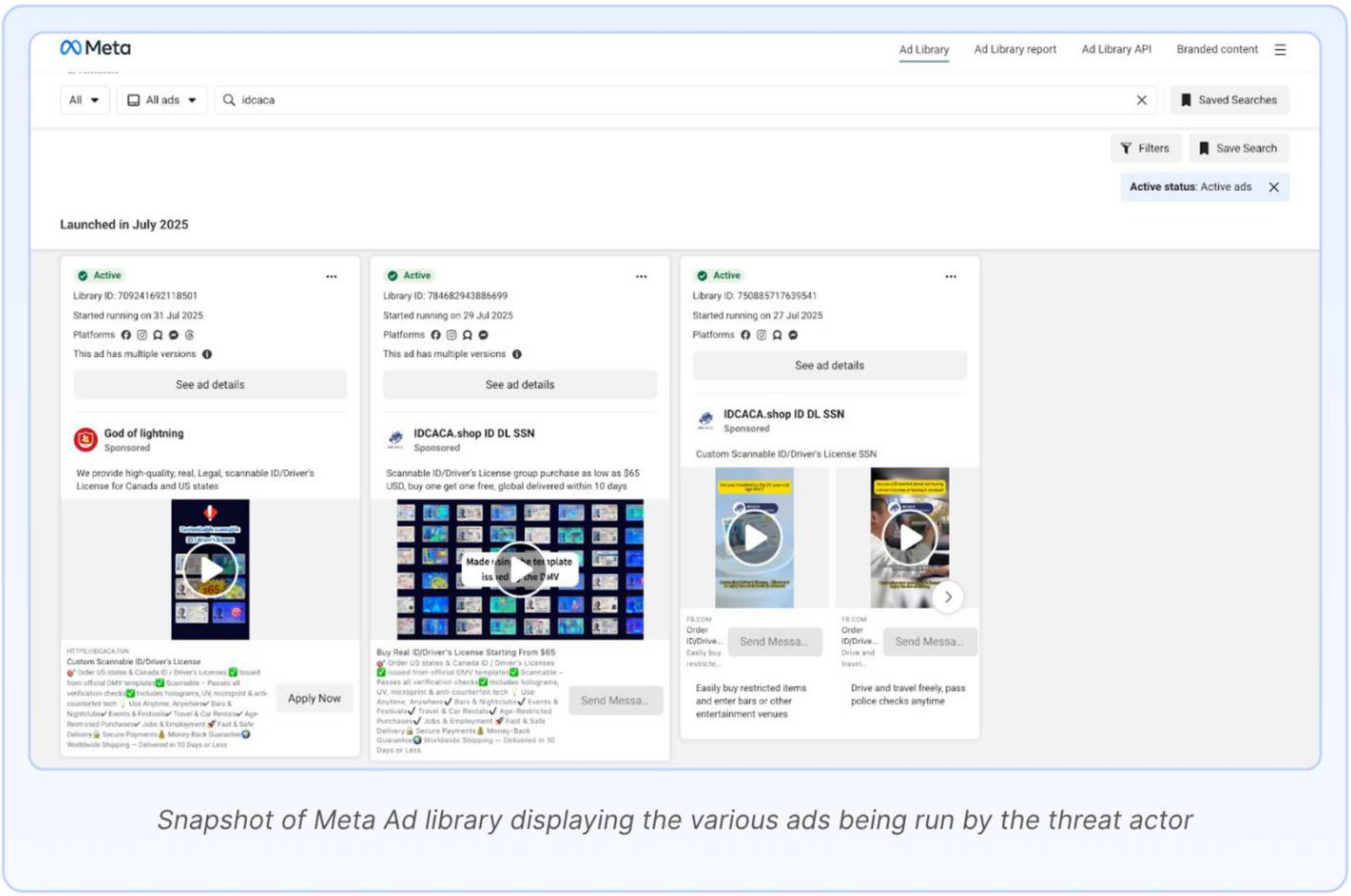
The primary method identified for promoting and distributing the fake licenses is through social media platforms. The threat actor operates **multiple accounts** across various platforms, regularly posting **advertisement videos** that showcase the features and uses of the counterfeit documents.

In addition to organic posts, the actor leverages **paid Meta Ads** to amplify reach across Facebook, Instagram, and other affiliated platforms, thereby ensuring consistent visibility among targeted audiences.

Many of these advertisements use **bold and enticing captions**, promoting illegal uses of the fake licenses, such as:

- "Use this card to buy restricted items and enter bars"
- "Drive and travel freely, pass police checks anytime"
- "Verify identity on platforms like 53Bank, Credit Union, Airbnb"
- "Claim benefits, medical aid, and employment proof"

These messages are deliberately crafted to appeal to individuals seeking to bypass legal or identity verification systems, highlighting the real-world risks and misuse potential of these fake documents.

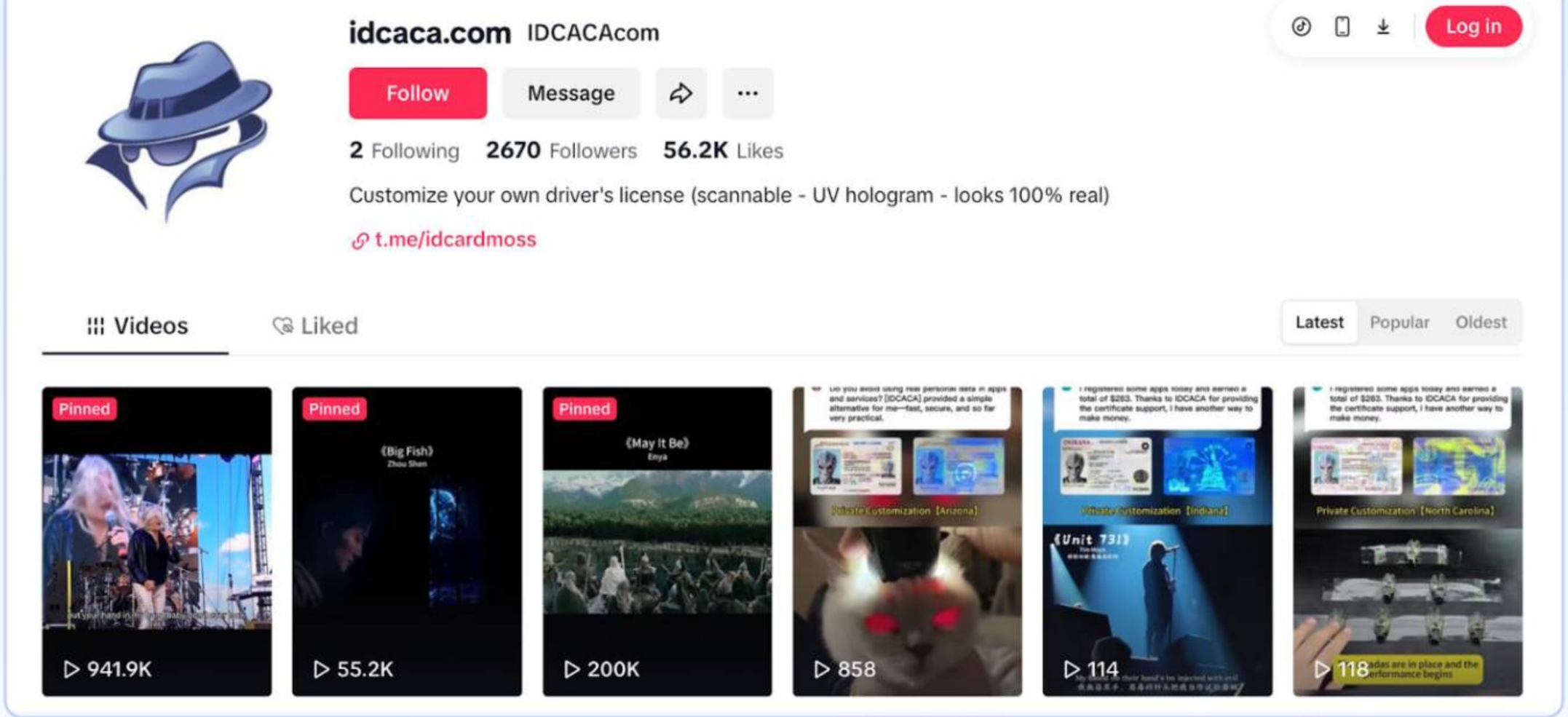


Snapshot of Meta Ad library displaying the various ads being run by the threat actor

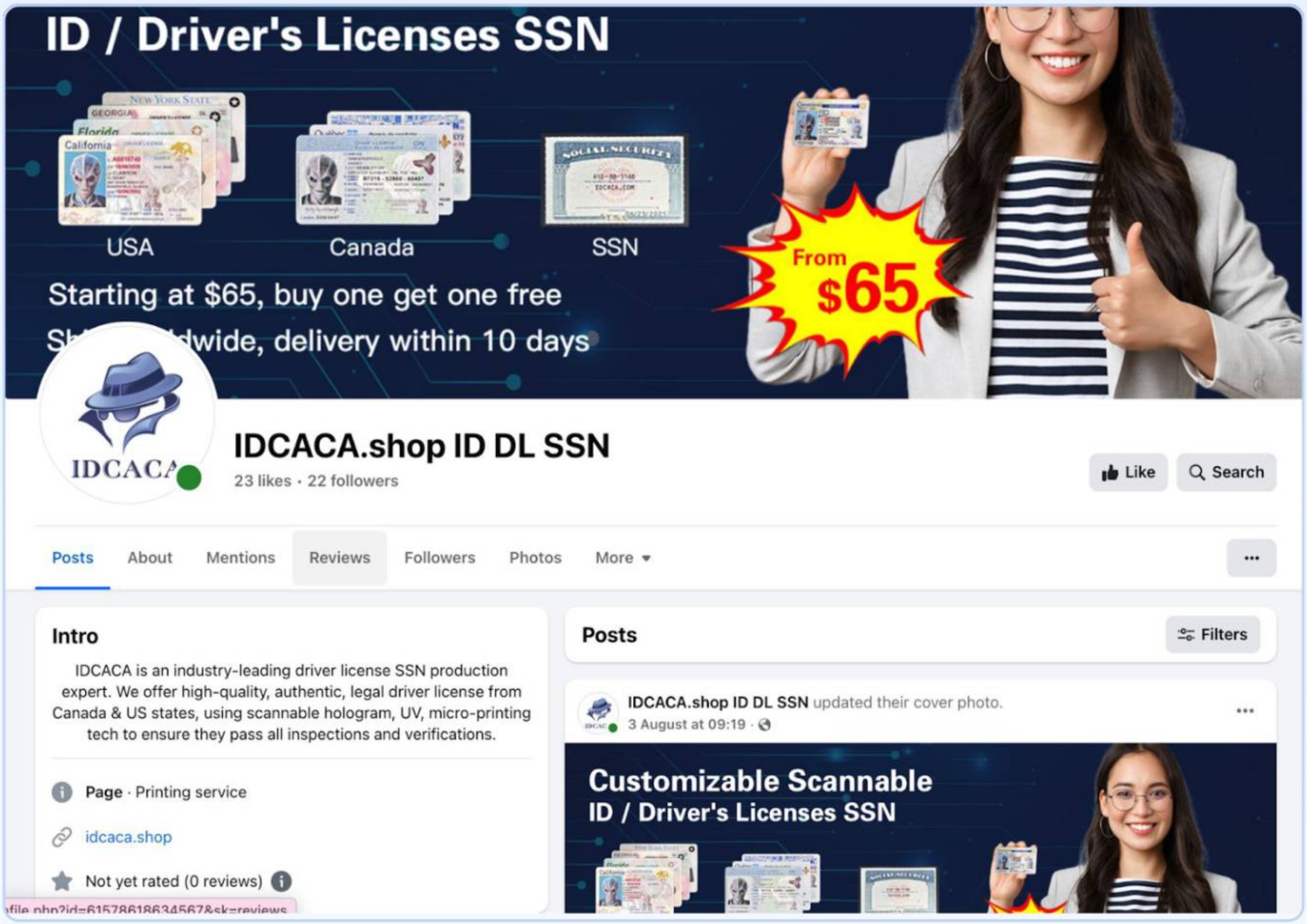
Social Media Handles

Below are a few of the social media accounts handled by the threat actor.

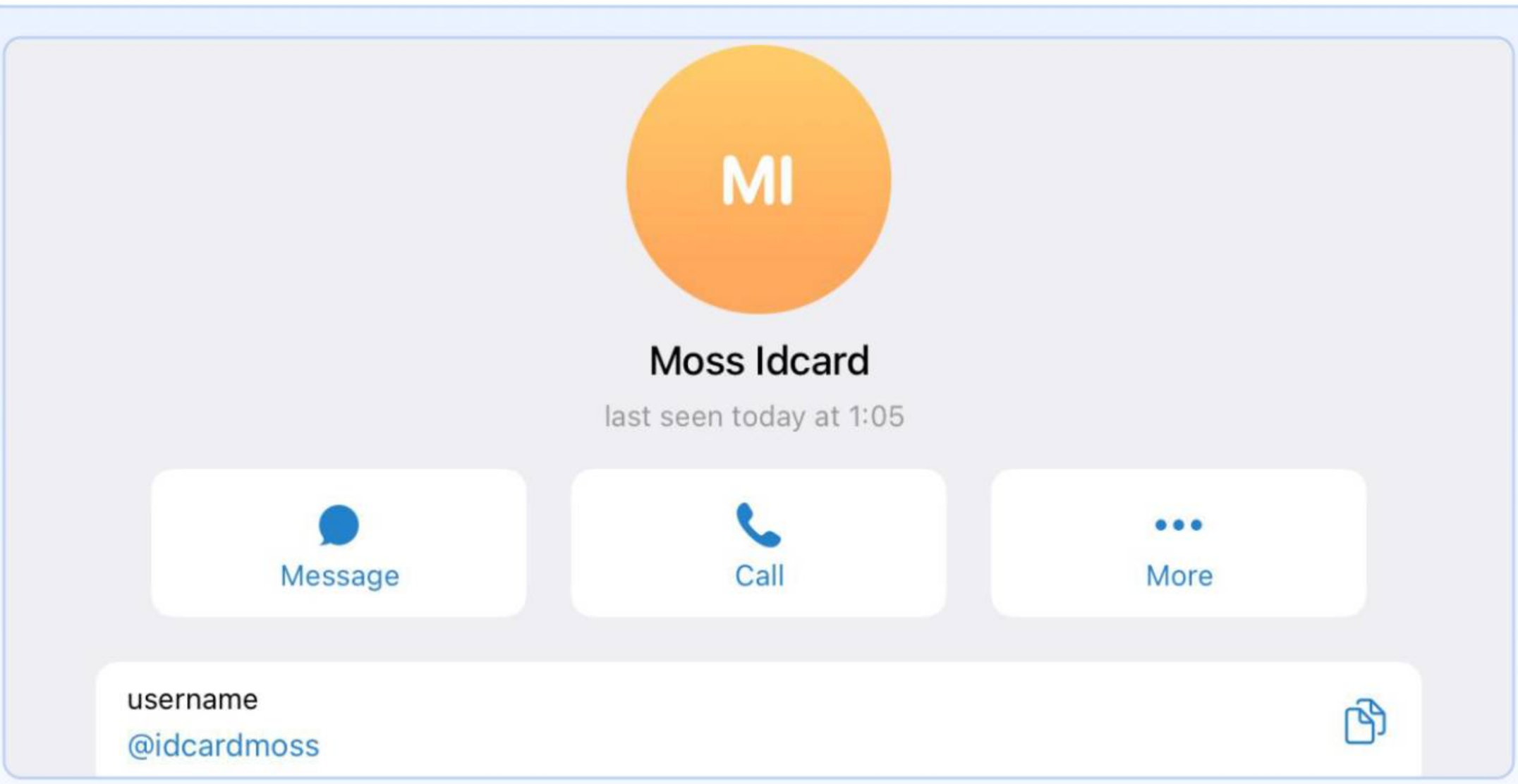
- **TikTok**
  - tiktok[.]com/@idcaca.com
- **Facebook**
  - facebook[.]com/profile.php?id=61577686345542
  - facebook[.]com/profile.php?id=61577760531879
  - facebook[.]com/profile.php?id=61578618634567
- **Youtube**
  - youtube[.]com/@IDCACA-DL
- **Telegram**
  - @idcardmoss
- **X (Twitter)**
  - x[.]com/topidcaca
  - x[.]com/CaliforniaDL_ID



Snapshot of the TikTok account owned by the threat actor



Snapshot of a Facebook page owned by the threat actor



Snapshot of the Telegram account of the threat actor used as the primary mode of communication

Tactics, Techniques, and Procedures - Overview

The complete operational workflow and tactics used by the threat actor, reveals a well-structured and coordinated fake ID distribution network. Below are the key Tactics, Techniques, and Procedures (TTPs) observed during the investigation :

Domain Control & Web Infrastructure : The threat actor maintains control of over 80+ domains, many with similar UI/UX. These sites function as fake storefronts offering services like counterfeit licenses, SSNs, and other identity documents.

Promotion & Traffic Generation : To lure buyers, the actor runs Meta Ads and spreads content across Telegram, WhatsApp, and other social platforms.

Order Funnel : Visitors are funneled into a structured order page where they submit detailed information including name, height, address, and custom data. Buyers choose shipping (standard/express) and production speed (normal/expedited), then proceed to payment.

Payment Handling : Diverse range of payment methods are used such as LianLian, PayPal, Debit/Credit Cards, Cryptocurrency etc. PayPal and credit/debit cards, often routed through fake e-commerce shell sites (e.g., accshop[.]life, cahomai[.]com), disguised as clothing or accessories stores.

Communication Channels : All pre or post-order interactions and updates happen over Telegram, WhatsApp, or WeChat-based live chat support embedded in the websites.

Manufacturing & Verification : Once payment is received, the threat actor sends order details to their production unit. A photo of the completed fake ID is shared with the buyer for confirmation before dispatch.

Stealth Packaging & Concealment : The ID is then hidden along with decoy items like purses or toys, and packed in cardboard boxes with internal cavities. A plastic camouflage sticker is applied to the card to evade detection during inspection. The buyer is sent a step-by-step tutorial video showing how to locate and retrieve the card from the package.

Shipping & Tracking : The final shipment is dispatched via multiple courier services such as FedEx, USPS ,Gofo, Canada Post, DHL etc and a tracking ID is shared within 2–3 days, allowing the buyer to monitor the delivery status.

Impact

National Security Threat : Fake driver's licenses allow criminals to bypass government ID checks at airports, transportation hubs, and border crossings. This poses a serious threat to national security as it enables the creation of alternate identities.

Underage Access to Restricted Goods & Services : These fake IDs are explicitly marketed to teenagers and minors, making it easier for them to illegally purchase alcohol, cigarettes or to gain entry into adult-only establishments such as bars, casinos, and clubs.

Abuse of Immigration and Border Systems : Undocumented migrants can use fake licenses to construct a false legal identity, secure employment, access housing, or move across state borders without detection.

SIM Swap and Financial Account Takeover : By using fake IDs to satisfy KYC checks, attackers can obtain SIM cards tied to victims' phone numbers. This enables SIM swap attacks, allowing access to sensitive bank accounts, cryptocurrency wallets, email, and two-factor authentication services, resulting in large-scale financial theft.

Pickup of Carded Goods : Fake licenses are commonly used as pickup verification documents for items purchased using stolen credit cards (carding). This lets cybercriminals collect high-value electronics, designer goods, or other items without revealing their true identity.

Mail-In Ballot & Voter Registration Fraud : As highlighted in recent FBI reports, fake identification has been used to fraudulently register voters or submit mail-in ballots, posing a serious threat to the integrity of democratic elections.

Evasion of Law Enforcement & Surveillance Systems : Criminals involved in fraud, trafficking, and organized crime use fake IDs to rent properties, buy SIM cards, rent vehicles, and conduct travel — all while staying off radar. This hinders surveillance efforts and makes long-term investigations significantly more difficult.

Welfare and Benefits Fraud : Fake licenses are exploited to fraudulently access government programs like unemployment benefits, food stamps, healthcare subsidies, and even COVID-era financial relief. This drains public resources and undermines trust in welfare systems.

Trust Abuse on Verified Platforms : Services like Airbnb, Uber, DoorDash, and online marketplaces rely on ID verification for user trust. Fake IDs allow malicious users to onboard fraudulently, conduct scams, or even endanger other users.

Recommendations

Immediate Domain Seizure and Infrastructure Takedown : LEAs, in collaboration with domain registrars and international cybercrime units, should work to seize and dismantle the 80+ domains linked to this operation.

Deploy Threat Intelligence Platforms for Continuous Monitoring : Platforms like CloudSEK XVigil can be actively used to detect, monitor, and attribute online infrastructure associated with fake ID distribution enabling early detection and disruption of similar threats at scale.

Use Exfiltrated Buyer Database for Criminal Investigations : The extracted buyer database contains personally identifiable information (PII) which can prove to be actionable intelligence. This should be used to Investigate end-users engaged in fraudulent activities, identify domestic collaborators or local distributors, if any.

Pursue Legal Action Against the Threat Actor : With high-confidence attribution including precise geolocation, webcam-captured facial imagery, and digital footprint, law enforcement can proceed with international legal collaboration. The extracted buyer database contains personally identifiable information (PII) which can prove to be actionable intelligence. This should be used to Investigate end-users engaged in fraudulent activities, identify domestic collaborators or local distributors, if any.

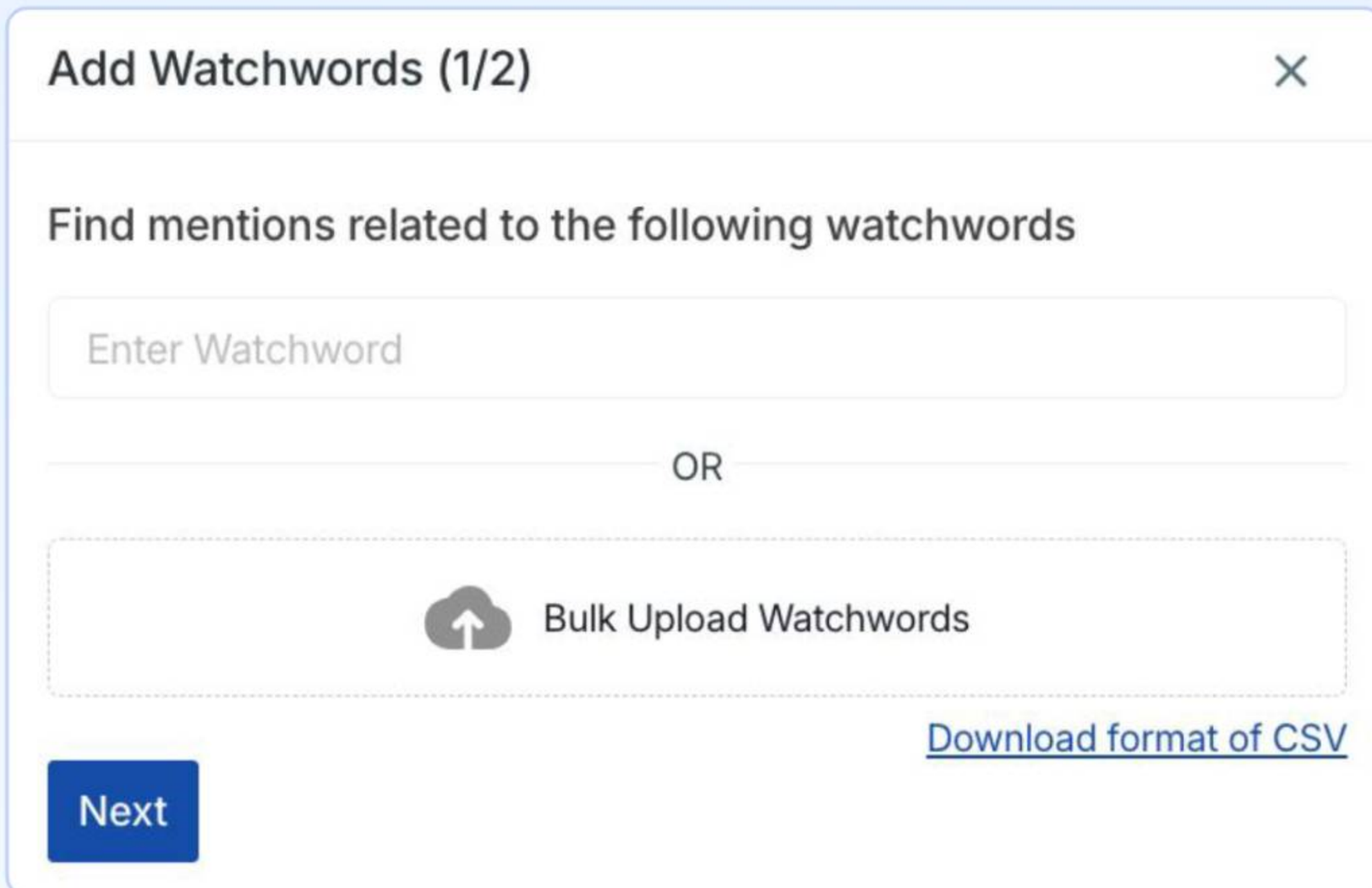
Collaborate with Courier Companies on Concealed Package Detection : Packaging methods uncovered should be shared with FedEx, USPS, UPS, DHL, etc., so they can flag and escalate suspicious parcels during inspection and transit.

Notify and Coordinate with Payment Processors for Traceability : Investigators should work with PayPal, Western Union, cryptocurrency platforms, and WooCommerce to trace transactions linked to this network. Freezing merchant accounts and following the money trail could yield crucial leads into domestic collaborators.

Use Delivery & Shipment Intel to Flag Suspicious Routes : The use of FedEx and USPS for shipping fake IDs globally reveals traceable logistics patterns. Law enforcement should correlate tracking IDs and suspicious shipping routes to intercept future shipments.

Leveraging CloudSEK Platform - XVigil

This investigation was significantly aided by the CloudSEK XVigil, Brand Threat Monitoring module, which provided end-to-end visibility across a wide range of digital sources. By configuring a targeted set of watchwords, XVigil enabled continuous monitoring across social media and messaging platforms, dark web, paste sites, and other online forums.



Snapshot displaying the "Add Watchwords" feature

By leveraging the added watchwords and logos, multiple domains linked to the threat actor were identified through XVigil's **Fake URLs and Phishing** module. This initial discovery served as the foundation for the broader investigation, enabling further pivots into the threat actor's operation.

Event Details

Module	Scan Date & Time
Fake URLs and Phishing	02 Aug, 2025 10:45:20 AM

Suspect URL

www.idcaca.com

Snapshot displaying an event under Fake URLs and Phishing module

Evidences / Screenshots

Snapshot displaying the evidence captured by the platform

By leveraging XVigil's **Fake Pages and Channels** module, it was possible to identify accounts operated by the threat actor across platforms such as TikTok, YouTube, Facebook, Instagram, and X. These sources provided valuable insights that helped track the threat actor's social media presence.

Event Details

Module
Fake Pages and Channels

Scan Date & Time
04 Aug, 2025 07:30:46 AM

Source Name
tiktok

Source URL
https://www.tiktok.com/@idcaca.com

Snapshot displaying an event under Fake Pages and Channels module

Evidences / Screenshots

Document Content

idcaca .com | IDCACAcom
Customize your own driver's license (scannable - UV hologram - looks 100% real)

Snapshot displaying the evidence and document content of the event

The platform's **Fake Pages & Channels** module was also useful in identifying Meta Ads that helped track the threat actor's advertising activities, and methods of propagation.

Event Details

Module
Fake Pages and Channels

Scan Date & Time
04 Aug, 2025 09:22:44 AM

Source Name
facebook

Source URL
https://www.facebook.com/ads/library/?id=750885717639541

Snapshot displaying an event under Fake Pages and Channels module

Evidences / Screenshots

Document Content

IDCACA .shop ID DL SSN | https://www.facebook.com/61578618634567/ | Custom Scannable ID/Driver's License SSN

Easily buy restricted items and enter bars or other entertainment venues

Drive and travel freely, pass police checks anytime

Easily verify identity on platforms like 53bank, credit union, Airbnb, etc.

Use fake IDs with confidence, avoid tracking

Easily claim benefits, medical aid, and employment proof | None | None | None | None

Snapshot displaying the evidence and document content of the event

This multi-layered approach, combining keyword-based detection along with HUMINT, OSINT and infrastructure testing enabled comprehensive mapping and profiling of the operation. This intelligence was crucial in understanding the tactics, reach, and operational structure of the actors behind the campaign.

Conclusion

This report highlights how a China-linked threat actor has built and sustained a large-scale counterfeit identity operation, enabling access to fake U.S. and Canadian licenses, along with SSN cards, through a complex, yet openly accessible infrastructure. This investigation offers a rare, inside look into the financial, technical, and operational depth of such campaigns. But this operation is just one of many. As these networks evolve and expand, disrupting them will require ongoing monitoring, deeper attribution, and coordinated action between law enforcement, platforms, and financial intermediaries, before counterfeit identity becomes a normalized gateway to digital and real-world crime.

CloudSEK

Predict | Protect | Quantify

CloudSEK is a Cyber Intelligence company offering Predictive Threat Analytics, Digital Risk Protection, Attack Surface and Supply Chain Monitoring, helping global organizations quantify and prioritize cyber threats for robust security.

Our Capabilities

- **Digital Risk Monitoring:** Real-time visibility and control over your digital assets.
- **External Attack Surface Monitoring:** Detect and mitigate vulnerabilities across 8+ Attack surfaces.
- **Third-party software & Supply Chain Monitoring:** Safeguard vendor ecosystems to prevent Supply chain breaches.
- **Cyber Threat Intelligence:** Proactively identify Indicators of Attack (IOAS) to stop threats in their tracks.
- **Cyber Risk Quantification:** Put a dollar value on potential threats to prioritize mitigation and demonstrate ROI.

95% Faster	80% Reduced	Zero	200+IAV
Threat Detection	Response time	False Positives	Use Cases

Why CloudSEK?

- **Predict Threats Before They Strike:** AI-driven intelligence to identify and mitigate threats at their source-before they become incidents.
- **Comprehensive Coverage:** Monitor 8+ attack surfaces and 200+ Initial Attack Vectors for full-spectrum visibility.
- **Contextual Intelligence:** Unified platform combines Cyber Intelligence, Brand Monitoring, Attack Surface Management, & Supply Chain Risk Analysis for actionable insights.

Trusted by Industry Leaders

NIC HCLTech HDFC BANK MetLife EMAAR & 300+ Organisation

ISO 9001 CERTIFIED

ISO 27001

#1 Threat Intelligence Vendor in APAC | Rated 4.8+ Gartner Peer Insights

aws Available in AWS Marketplace

GDPR COMPLIANT

info@cloudsek.com

www.cloudsek.com

Scan QR to Book a Demo