Investigation Report: UnionPay-Impersonation Phishing Infrastructure

Vincent Yang
OwO Network, LLC / NOC

6 May 2026

Prepared as a formal incident investigation report

Abstract

This report documents a high-confidence payment-card phishing incident in which SMS messages impersonating China UnionPay directed the victim to https://up.cnpayglobal.com/. The incident occurred shortly after a payment activity near 〒 104-0061 Tokyo, Chuo City, Ginza, 3 Chome-3-13, at approximately 35.6728586, 139.7624018. The phishing website collected payment-card verification data and SMS one-time passwords. After the interaction, the victim received bank verification messages for an attempted online payment of CNY 11,987.95. The victim also observed that the verification-code request remained in a loading state for approximately one to two minutes, which is consistent with a live-relay workflow and may indicate manual downstream use of the submitted card details. That interpretation remains an investigative hypothesis, not a confirmed fact. Technical investigation links the observed lure domain and related infrastructure to a domain cluster hosted on `104.225.145.101`, associated with IT7 Networks Inc and AS25820. The phishing site also showed implementation characteristics consistent with a Vite.js-built web application. RDAP records show consistent use of NameSilo, DNSOWL nameservers, and PrivacyGuardian privacy protection across the domain cluster.

Keywords: phishing; UnionPay impersonation; SMS spoofing; payment-card fraud; RDAP; NameSilo; AS25820

1 Incident Overview

Table 1: Case metadata

Field	Value
Report date	2026-05-06
Incident date / time window	2026-05-05, shortly after a local payment activity; bank verification SMS messages followed later the same day, based on victim-device local time
Incident location	Near 〒 104-0061 Tokyo, Chuo City, Ginza, 3 Chome-3-13; coordinates 35.6728586, 139.7624018
Primary phishing URL	https://up.cnpayglobal.com/
Root domain	`cnpayglobal.com`
Observed hosting IP	`104.225.145.101`
Network / ASN	IT7 Networks Inc / AS25820
Asset source	`749079eec0_202605060859` asset-data CSV
RDAP query time	2026-05-06 16:12 UTC

Shortly after a payment activity near 〒 104-0061 Tokyo, Chuo City, Ginza, 3 Chome-3-13, the victim received SMS messages impersonating China UnionPay. The message claimed that the

victim's overseas payment capability had been disabled and instructed the victim to re-authenticate through https://up.cnpayglobal.com/. The destination website presented a UnionPay-themed card authentication interface and requested sensitive cardholder information, including card number, CVV/CVN2, expiration date, mobile phone number, and SMS verification code.

After the victim selected the verification-code function, the page remained in a loading state for approximately one to two minutes. This delay is consistent with a live-relay or operator-assisted fraud workflow. One plausible hypothesis is that the backend operators were manually entering the submitted card details into a downstream purchase flow, such as airline-ticket or hotel booking purchases sometimes associated with low-price proxy-purchase fraud. This is an inference from the observed behavior and subsequent bank payment SMS, not direct proof of the downstream merchant or purchase category.

The phishing interface displayed an English option in the upper-right corner, but the victim observed that clicking it had no effect. The non-functional language switch, combined with the Chinese-language SMS lure and UnionPay-themed page content, supports the assessment that the campaign primarily targeted Chinese-speaking UnionPay cardholders physically present in Japan.

The timing, location, and spoofed sender identity are consistent with suspected SMS sender spoofing or pseudo-base-station activity. This remains an inference based on victim-side evidence. Carrier-side records or law-enforcement telecom records would be required to conclusively identify the SMS delivery mechanism.

2 Evidence

The following screenshots are primary victim-side evidence. They document the SMS lure, bank verification messages, phishing landing page, and credential collection form.

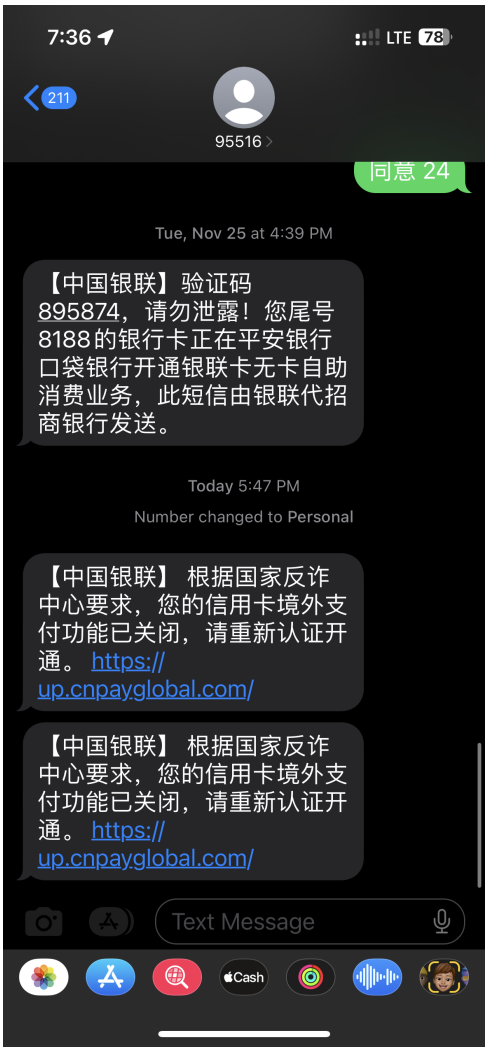

Figure 1: Spoofed UnionPay SMS lure containing `https://up.cnpayglobal.com/`.

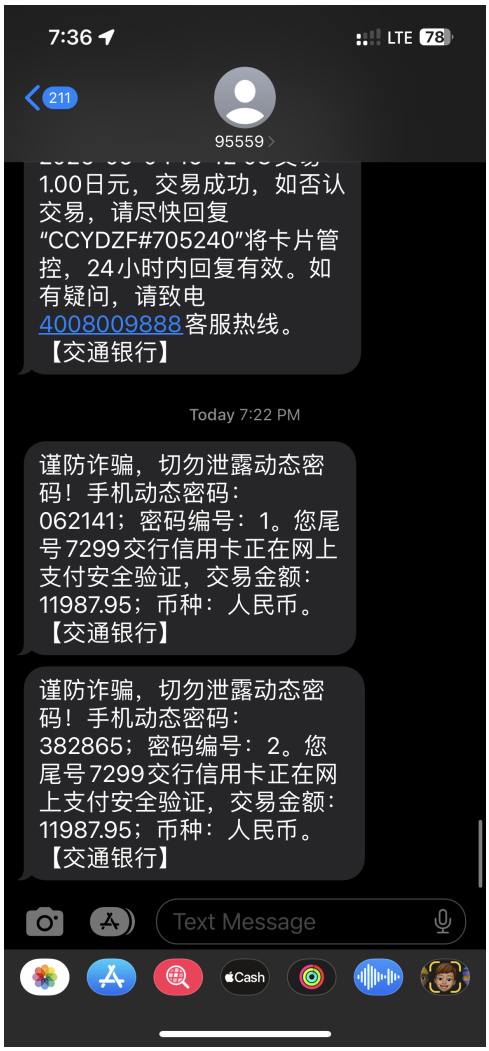

Figure 2: Bank SMS verification messages for an attempted online payment of CNY 11,987.95.

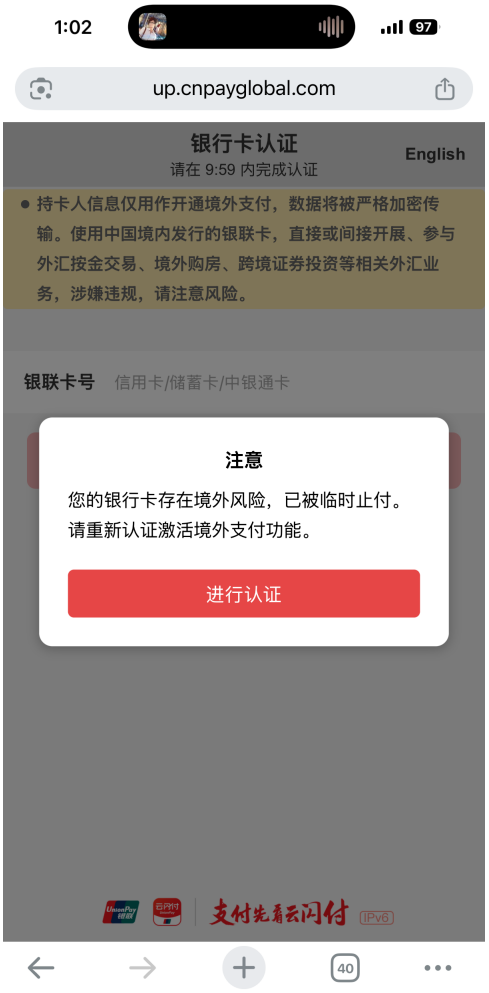

Figure 3: Phishing landing page showing a UnionPay-style card authentication prompt.

Figure 4: Credential and OTP harvesting form requesting CVN2/CVV, expiration date, mobile number, and SMS code.

3 Attack Chain Analysis

The observed attack chain is assessed as follows:

1. The victim completed a payment activity near 〒 104-0061 Tokyo, Chuo City, Ginza, 3 Chome-3-13.
2. The victim received SMS messages impersonating China UnionPay.
3. The SMS messages directed the victim to `https://up.cnpayglobal.com/`.
4. The phishing page requested full card verification data and SMS OTP.

5. The verification-code request remained in a loading state for approximately one to two minutes, suggesting possible live relay or operator-assisted backend interaction with a real payment workflow.

6. A plausible investigative hypothesis is that the submitted card details were being manually used for downstream purchases, such as airline-ticket or hotel bookings; this has not been independently confirmed.

7. The upper-right English option on the phishing page was non-functional, suggesting the workflow was designed primarily for Chinese-speaking users in Japan.

8. The victim received bank verification messages for an attempted CNY 11,987.95 online payment.

9. The victim identified the website as phishing and reported it to the registrar, registry, and hosting network.

4 Infrastructure Indicators

4.1 Primary Indicators

Table 2: Primary indicators of compromise

Indicator	Value
Primary lure host	`up.cnpayglobal.com`
Root domain	`cnpayglobal.com`
Hosting IP	`104.225.145.101`
Observed web build framework	Vite.js
ASN	`AS25820`
Network name	IT7NET
Registrar	NameSilo, LLC
Registrar IANA ID	1479
Registrar abuse contact	`abuse@namesilo.com`
IP/ASN abuse contact	`abuse@sioru.com`
Nameservers	`NS1.DNSOWL.COM`; `NS2.DNSOWL.COM`; `NS3.DNSOWL.COM`

4.2 FOFA Asset Data

The supplied asset file contains 27 rows including the header. The deduplicated related hosts observed on `104.225.145.101` are summarized below. The source title translates to “Bank Card Authentication.”

Table 3: FOFA-derived phishing infrastructure on `104.225.145.101`

Host	Port(s)	Page title	Root domain
`cn.lianhezf.com`	80 / 443	Bank Card Authentication	`lianhezf.com`
`cn.up-hwrz.com`	80 / 443	Bank Card Authentication	`up-hwrz.com`
`cn.yinlianasia.com`	80 / 443	Bank Card Authentication	`yinlianasia.com`
`cn.uphwzf.com`	80 / 443	Bank Card Authentication	`uphwzf.com`
`cn.yinlianworld.com`	80 / 443	Bank Card Authentication	`yinlianworld.com`
`cn.jingwaizf.com`	80 / 443	Bank Card Authentication	`jingwaizf.com`
`zgyinlian-zf.com`	80 / 443	Bank Card Authentication / 400	`zgyinlian-zf.com`
`cn.uprenzheng.com`	80 / 443	Bank Card Authentication	`uprenzheng.com`
`cn.upjprz.com`	80 / 443	Bank Card Authentication	`upjprz.com`
`zhifu-oversea.com`; `cn.zhifu-oversea.com`	80 / 443	Bank Card Authentication / blank	`zhifu-oversea.com`
`104.225.145.101`	80 / 443 / 888 / 22	Bank Card Authentication / 400 / 403	N/A

5 RDAP and WHOIS Findings

Registry dates in Table 4 are based on Verisign RDAP unless otherwise noted. Registrar-side dates may differ by one calendar day because NameSilo reports normalized registrar dates separately from the Verisign timestamp.

Table 4: Domain RDAP summary

Domain	Status at query time	Registration	Expiration
cnpayglobal.com	client transfer prohibited	2026-05-05 01:35:56 UTC	2027-05-05 01:35:56 UTC
lianhezf.com	client transfer prohibited	2026-04-02 03:45:27 UTC	2027-04-02 03:45:27 UTC
up-hwrz.com	client transfer prohibited	2025-12-20 05:55:48 UTC	2026-12-20 05:55:48 UTC
yinlianasia.com	client hold; client transfer prohibited	2026-04-21 03:27:59 UTC	2027-04-21 03:27:59 UTC
uphwzf.com	client transfer prohibited	2025-12-25 08:15:20 UTC	2026-12-25 08:15:20 UTC
yinlianworld.com	client hold; client transfer prohibited	2026-04-04 03:08:18 UTC	2027-04-04 03:08:18 UTC
jingwaizf.com	client hold; client transfer prohibited	2025-11-19 08:25:35 UTC	2026-11-19 08:25:35 UTC
zgyinlian-zf.com	client transfer prohibited	2025-11-22 17:22:02 UTC	2026-11-22 17:22:02 UTC
uprenzheng.com	client hold; client transfer prohibited	2025-12-13 04:15:48 UTC	2026-12-13 04:15:48 UTC
upjprz.com	client hold; client transfer prohibited	2025-12-13 04:24:00 UTC	2026-12-13 04:24:00 UTC
zhifu-oversea.com	client hold; client transfer prohibited	2025-12-06 03:07:12 UTC	2026-12-06 03:07:12 UTC

Table 5: Common registrar and DNS pattern

Field	Observed value
Registrar	NameSilo, LLC
Registrar IANA ID	1479
Registrar support	support@namesilo.com
Registrar abuse	abuse@namesilo.com; +1.480.524.0066
Privacy service	PrivacyGuardian.org / See PrivacyGuardian.org
Common privacy phone	+1.3478717726
DNS provider	DNSOWL
DNSSEC	Not delegation-signed

Table 6: Hosting RDAP summary for `104.225.145.101`

Field	Value
Network handle	`NET-104-225-144-0-2`
Address range	`104.225.144.0`–`104.225.159.255`
Network name	`CL-104-225-144-0-20`
Type / status	Assignment / active
IP registrant entity	IT7 Networks Inc
IP registrant address	530 W 6th Street, Los Angeles, CA 90014, United States
Related registrant	Cluster Logic Inc
Abuse contact	`abuse@sioru.com`; +1-408-260-5757
NOC / technical / administrative	`arin-noc@sioru.com`; `arin-tech@sioru.com`; `arin-admin@sioru.com`

Table 7: Hosting RDAP summary for AS25820

Field	Value
AS number	`AS25820`
AS name	IT7NET
Status	Active
Registrant	IT7 Networks Inc
Registrant address	4974 Kingsway Ave, Suite 668, Burnaby, BC V5H 4M9, Canada
Abuse contact	`abuse@sioru.com`; +1-408-260-5757
NOC / technical / administrative	`arin-noc@sioru.com`; `arin-tech@sioru.com`; `arin-admin@sioru.com`

6 Assessment

This incident is assessed as a high-confidence UnionPay-themed payment-card phishing campaign. The conclusion is supported by the following observations:

1. The SMS impersonates China UnionPay and directs the victim to a non-official, newly registered domain.
2. `cnpayglobal.com` was registered on 2026-05-05, matching the incident window.
3. The phishing page requests CVV/CVN2, expiration date, phone number, and SMS verification code.
4. A real bank payment verification SMS for CNY 11,987.95 followed the interaction.

5. The one-to-two-minute verification-code delay is consistent with a live-relay workflow and may indicate operator-assisted downstream purchase attempts.
6. The non-functional English option and Chinese-language interaction path support a target profile of Chinese-speaking UnionPay users in Japan.
7. The phishing website appears to have been implemented as a Vite.js-built web application, which provides a useful technical fingerprint for log searches, file-system triage, and related-site clustering.
8. FOFA asset data identifies many similarly themed "Bank Card Authentication" hosts on the same IP address.
9. RDAP records demonstrate strong infrastructure overlap across registrar, DNS provider, privacy service, and hosting IP.
10. Several related domains already show `client hold`, suggesting prior abuse handling or takedown activity against the same cluster.

7 Actions Already Taken

The victim has already reported `cnpayglobal.com` to NameSilo and requested suspension of all DNS resolution. The matter has also been submitted to Verisign as the `.com` registry. The AS25820 / IT7 Networks abuse contact identified through RDAP has also been contacted.

8 Recommended Actions

NameSilo and Verisign should be requested to apply `client hold` or an equivalent suspension to `cnpayglobal.com`, review and suspend related domains, preserve registration/account/DNS logs, correlate PrivacyGuardian and NameSilo account metadata, and search for additional domains registered through the same account, payment method, login IP history, or privacy profile.

IT7 Networks, Cluster Logic, and AS25820 should be requested to disable the phishing content on `104.225.145.101`, preserve web server logs, reverse proxy logs, SSH logs, control-panel logs, operator-panel logs, browser-automation traces, downstream order-submission logs, customer records, and payment records, identify and suspend the customer controlling the host, and search adjacent network space for similar UnionPay or overseas-payment phishing content. Because the site appears to use Vite.js, responders should also search for Vite build artifacts, hashed JavaScript

and CSS assets, source-map remnants, and deployment paths that may link this site to other related hosts.

The exposed card should be treated as compromised if card number, CVV/CVN2, expiration date, mobile number, or OTP were entered. The card issuer should replace the card, block online, overseas, and card-not-present transactions until replacement, and preserve risk and authorization logs for the attempted CNY 11,987.95 payment, including merchant descriptors, device fingerprints, transaction-channel metadata, and any airline, hotel, or travel-merchant indicators if present. The mobile carrier should be asked to investigate sender spoofing or pseudo-base-station activity near the Ginza location during the relevant time window.

9 Conclusion

The collected SMS evidence, phishing-page screenshots, FOFA asset data, RDAP records, and Vite.js implementation fingerprint together support the conclusion that `up.cnpayglobal.com` and the related domains constitute coordinated payment-card phishing infrastructure impersonating China UnionPay. The one-to-two-minute verification-code delay and the non-functional English option further support a live-relay fraud workflow aimed at Chinese-speaking UnionPay cardholders in Japan. Immediate takedown, log preservation, and cross-provider correlation are warranted.

A English Takedown List

`up.cnpayglobal.com`
`cnpayglobal.com`
`cn.lianhezf.com`
`cn.up-hwrz.com`
`cn.yinlianasia.com`
`cn.uphwzf.com`
`cn.yinlianworld.com`
`cn.jingwaizf.com`
`zgyinlian-zf.com`
`cn.uprenzheng.com`
`cn.upjprz.com`
`zhifu-oversea.com`
`cn.zhifu-oversea.com`
`104.225.145.101`