Sealed

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CIVIL ACTION NO.

MICROSOFT CORPORATION, H2 PHARMA LLC, and GATEHOUSE DOCK CONDOMINIUM ASSOCIATION

Plaintiffs,

v.

DOES 1-7

Defendants

FILED UNDER SEAL

DECLARATION OF MAURICE MASON IN SUPPORT OF PLAINTIFFS' MOTION FOR TEMPORARY RESTRAINING ORDER AND RELATED RELIEF

I, Maurice Mason, declare as follows:

1. I am a Principal investigator in Microsoft Corporation's Digital Crimes Unit ("DCU"). I make this declaration based upon my personal knowledge, and upon information and belief based on my review of documents and evidence collected during Microsoft's investigation and civil discovery in this action.

2. I have been employed by Microsoft since August 2021. In my role, I assess technological security threats to Microsoft and the impact of such threats on Microsoft's business and customers. Among my responsibilities is protecting Microsoft's online service assets from network-based attacks. Prior to my current role, I worked as a Senior Consultant on Microsoft's Incident Response Team, where I was a lead digital forensic analyst managing multiple incident response and threat-hunting engagements that included performing incident response and forensic analysis for Fortune 500, Fortune 100, and Fortune 50 companies. Prior to joining

Microsoft, I held various positions, both in the private sector and in government, where I performed digital forensic analysis, including on malware and ransomware-related matters.

3. I am one of the persons at Microsoft responsible for assisting with the investigation into piracy of Microsoft software by an entity known as RedVDS. My work investigating RedVDS has included collaboration with my colleagues Sean Ensz and Donal Keating. I am familiar with the contents of the declarations they are submitting in this case.

RedVDS Test Buys

4. The RedVDS Enterprise engages the services of other third-party hosting providers and installs unauthorized copies of Windows Server on those hosting providers' servers, including within the United States. The RedVDS Enterprise then sells access to these copies of Windows Server to end users at a rate between $24 to $80 per month, depending on storage, CPU, and memory preferences. The RedVDS Enterprise maintains and uses a significant number of active virtual servers monthly. These servers are predominately used by cybercriminals, facilitating a wide range of illicit activities targeting Microsoft and its customers. Microsoft's Digital Crimes Unit has linked RedVDS infrastructure to numerous security incidents and has determined that RedVDS is a significant and persistent enabler of attacks against users of Microsoft's operating systems, communications services, and cloud computing services

5. I directed multiple test buys of the RedVDS service as part of my work investigating RedVDS. I began this process by accessing the RedVDS Enterprise website, where I anonymously registered and created an account. **Figures 1-3** depict the user interface I encountered during the first steps of the test buy process.

Fig. 1

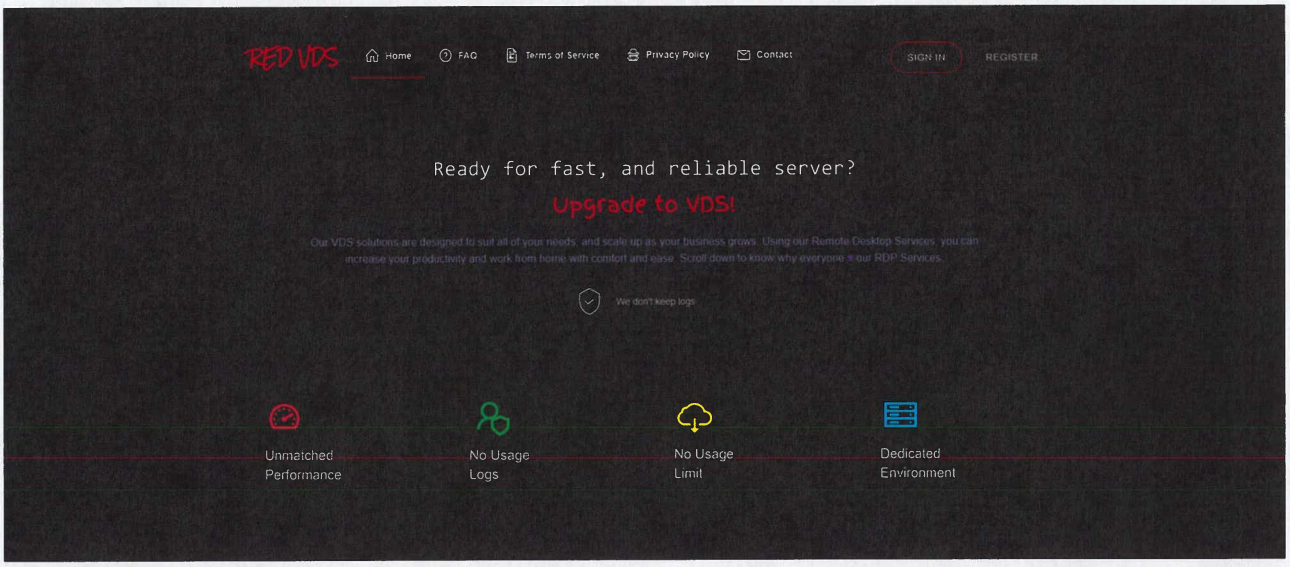

RED VDS
Home
FAQ
Terms of Service
Privacy Policy
Contact
SIGN IN
REGISTER
Ready for fast, and reliable server?
Upgrade to VDS!
Our VDS solutions are designed to suit all of your needs, and scale up as your business grows. Using our Remote Desktop Services, you can increase your productivity and work from home with comfort and ease. Scroll down to know why everyone ♥ our RDP Services.
We don't keep logs
Unmatched Performance
No Usage Logs
No Usage Limit
Dedicated Environment

Fig. 2

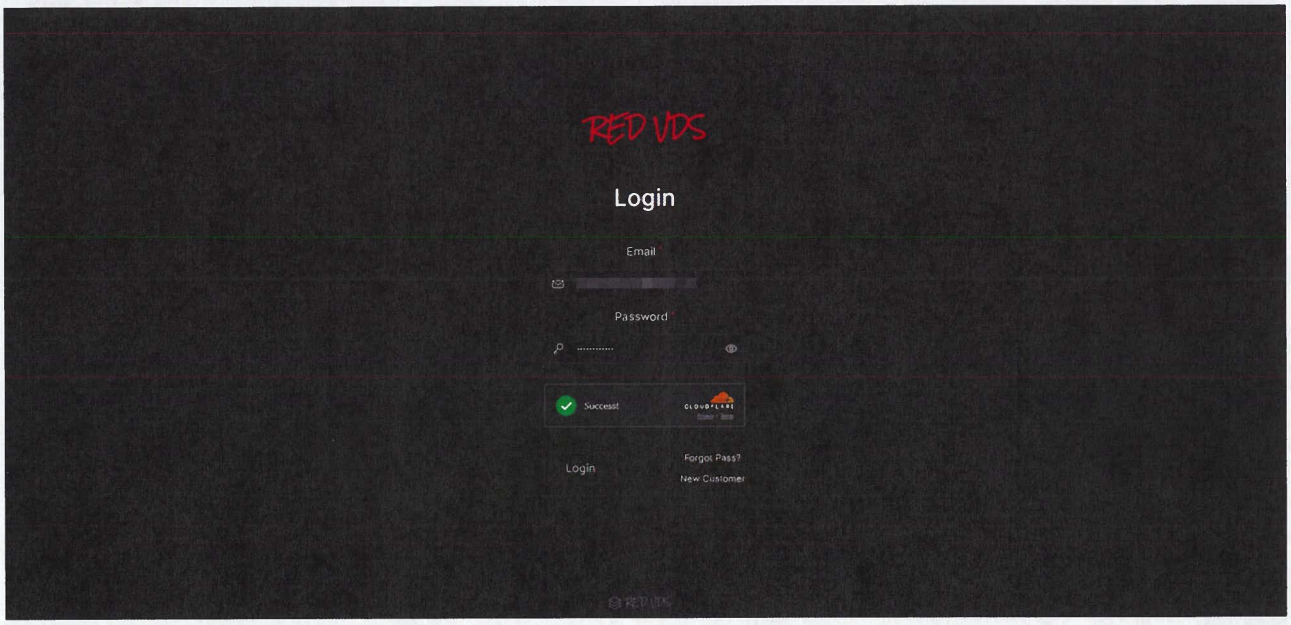
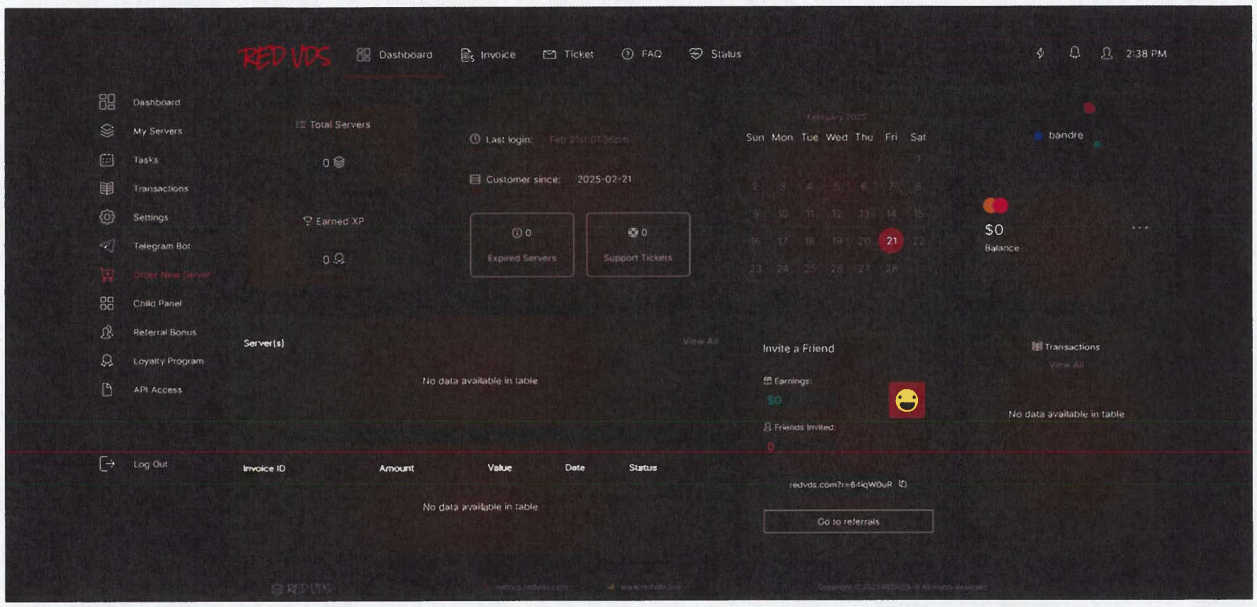

RED VDS
Login
Email
Password
Success!
Login
Forgot Pass?
New Customer

Fig. 3



6. Next, I reviewed the range of virtual desktop plans offered on the platform. These plans featured multiple configuration options, allowing customization of key specifications such as CPU cores, RAM capacity, and storage size to meet specific performance requirements as show in in **Figure 4** below.

Fig. 4

7. After selecting the desired specifications, I was directed to a product page that outlined the terms of service and detailed information about the chosen Windows Server configuration. To complete the purchase, the platform generated an invoice page featuring a QR code linked to a Bitcoin (BTC)[1] address. Customers could either scan the QR code or copy the BTC address to initiate and finalize the payment, as shown in **Figure 5** and **Figure 6** below.

[1] Bitcoin is a decentralized cryptocurrency that operates a public distributed ledger of transactions, which is referred to as a "blockchain."

Fig. 5

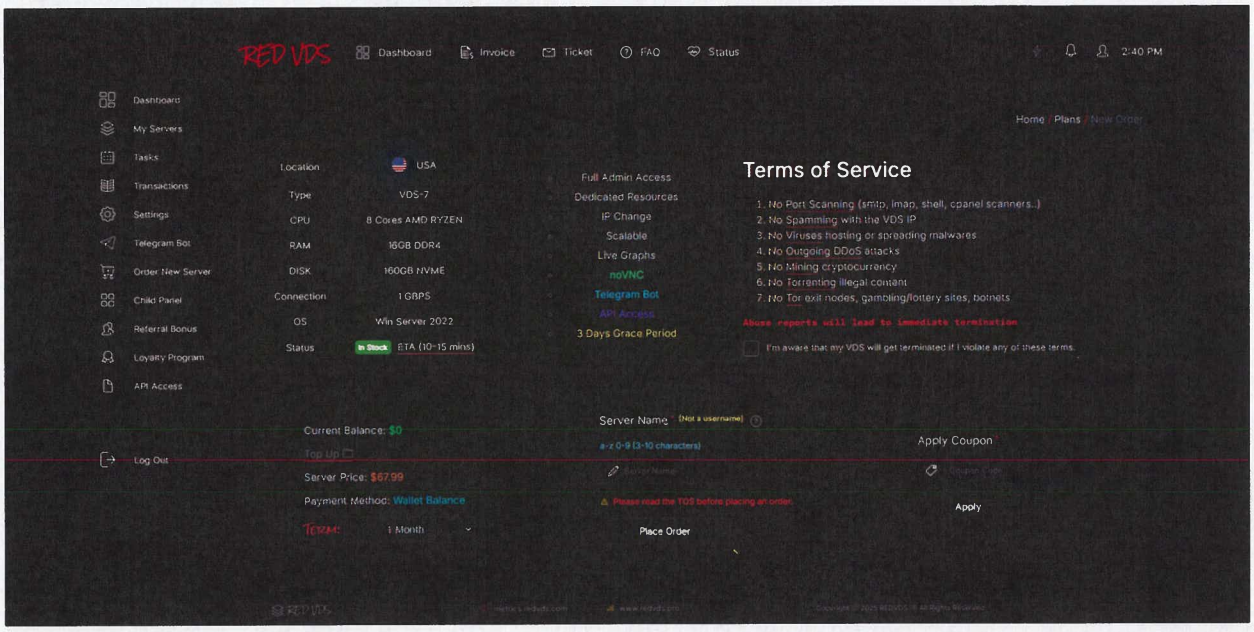
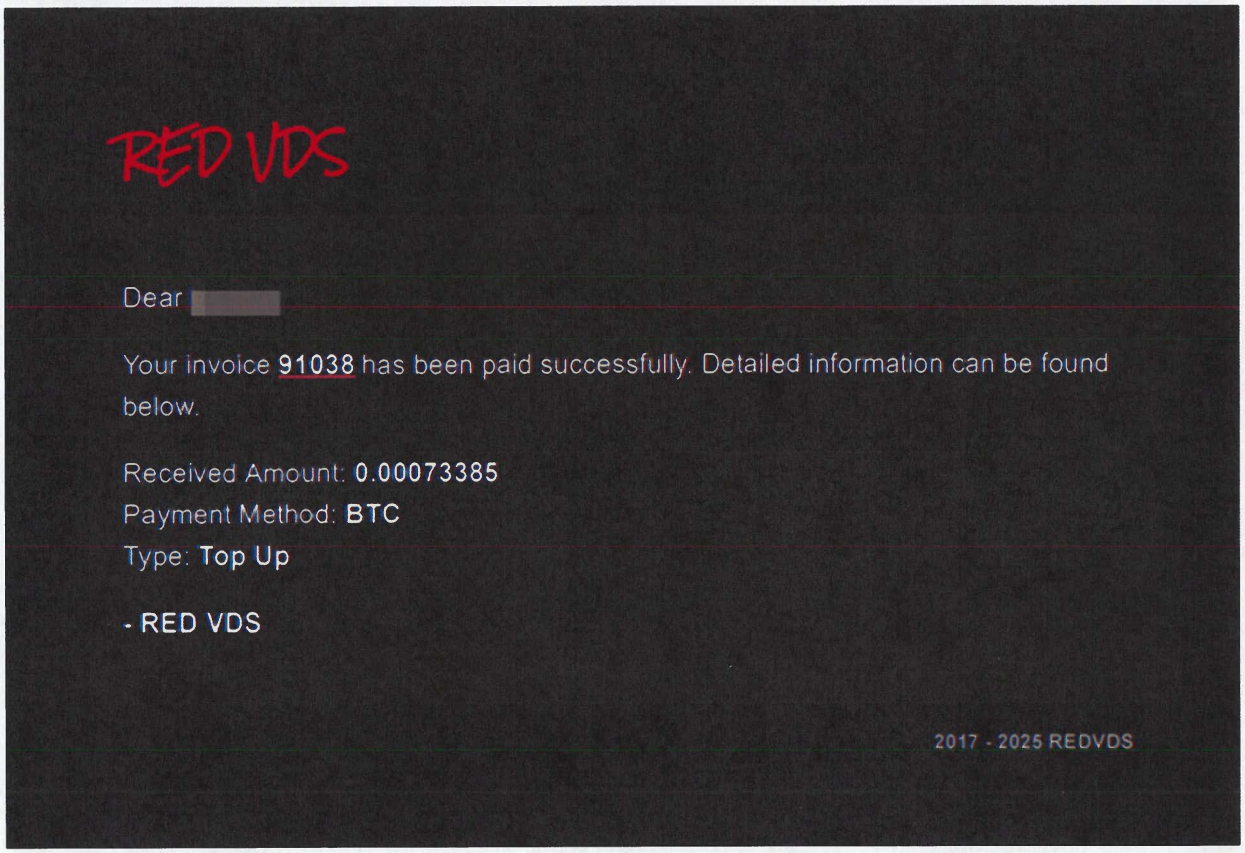


Fig. 6

8. I observed that after receiving payment, the RedVDS Enterprise deploys an automated process to create a virtual machine for the end user using the image and copy of Windows Server 2022 discussed above. End users then use the virtual machine image, Windows

Server software, and hosting services provided by the RedVDS Enterprise to remotely access and control virtual computers, commonly for malicious purposes. **Figure 7** below depicts the conclusion of the payment flow.

Fig. 7



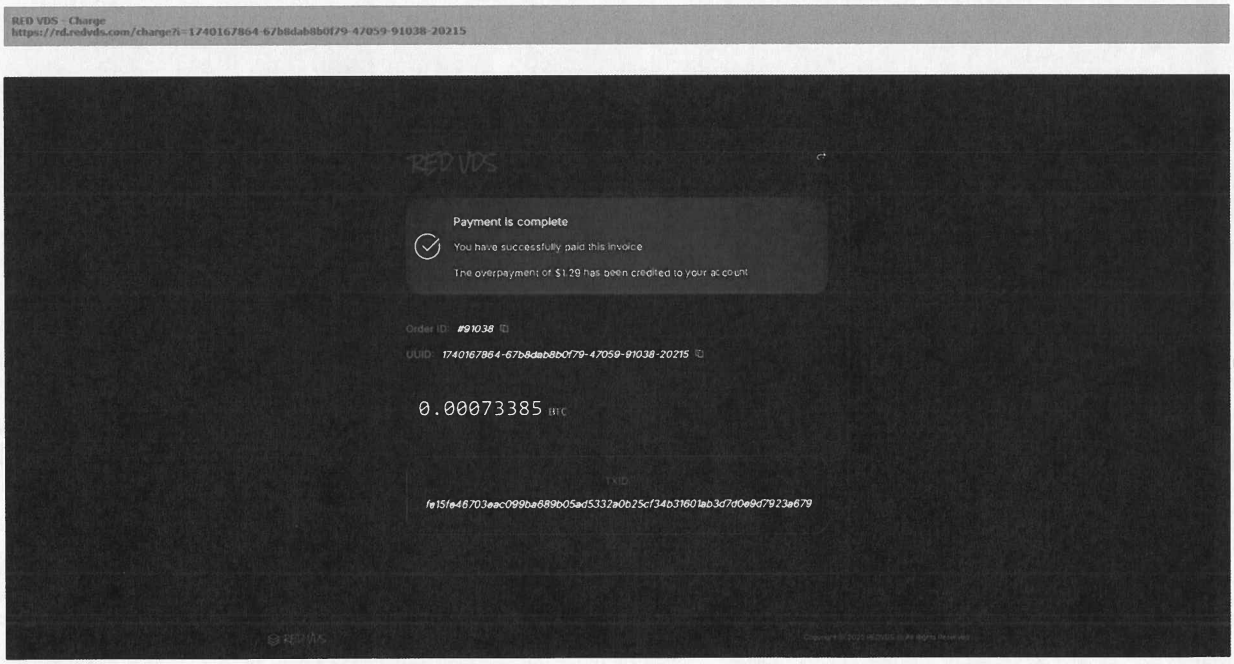
Blockchain Analysis

9. As described herein, I used the cryptocurrency account information provided to me by RedVDS Defendants to conduct a further financial analysis of the transactions and the cryptocurrency wallets used by the RedVDS Enterprise. I conducted this analysis using the information RedVDS Defendants provided to me, open-source information, and Chainalysis Reactor, a blockchain intelligence tool that facilitates the tracing of cryptocurrency funds.

10. Chainalysis Reactor groups ("clusters") cryptocurrency addresses that are controlled by the same entity ("clustering") and then ties those clusters to specific real-world entities based on information gleaned from other sources. Those sources amass information regarding cryptocurrency addresses through test transactions, open source-intelligence (OSINT), collecting and verifying evidence from third parties that have conducted transactions with entities on the blockchain, and exchanging information with law enforcement agencies ("attribution").

11. On February 21, 2025, I completed a purchase from RedVDS Enterprise for a copy of a Windows Server. Prior to the transaction, I demonstrated intent to engage with the platform by creating an account and registering on RedVDS.com. Payment was made in BTC to the RedVDS Defendants, and I received a receipt confirming the transaction, which included the corresponding transaction hash[2] as verification of the purchase. See **Figure 8** below.

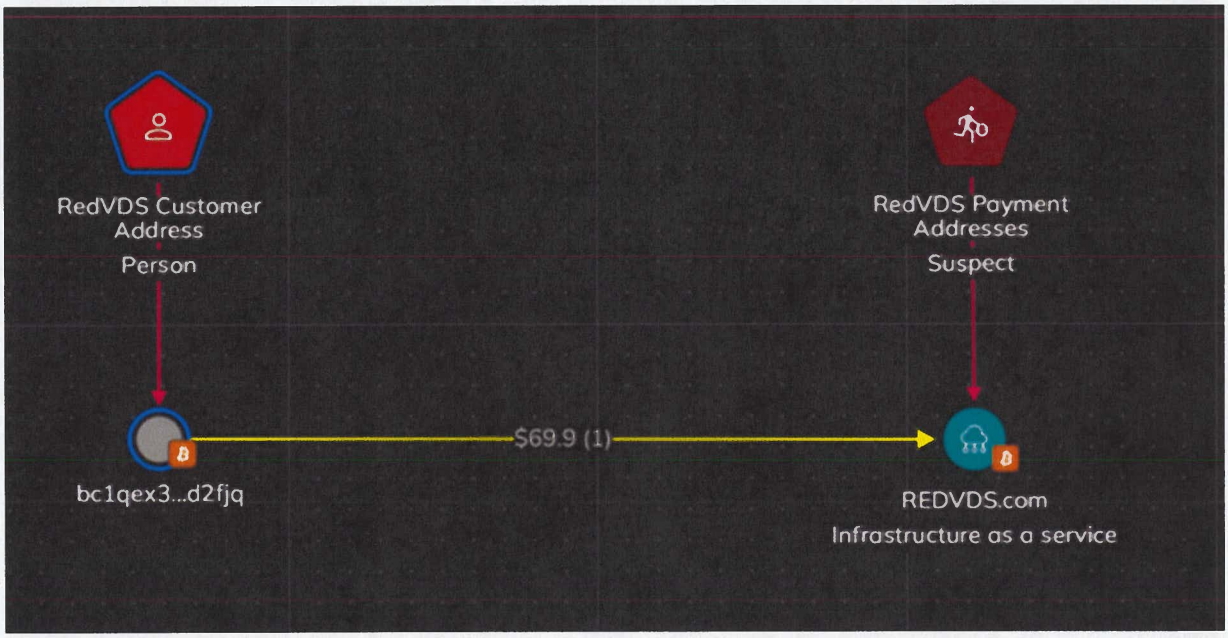
Fig. 8



[2] Transaction Hash is a unique identifier assigned to every transaction on the blockchain, serving as a digital receipt that allows users to track and verify their transactions."

12. Using Chainalysis Reactor, I conducted an analysis of transaction hash fe15fe46703eac099ba689b05ad5332a0b25cf34b31601ab3d7d0e9d7923a679, which was linked to the acquisition of a RedVDS server. My analysis revealed that the receiving BTC address, bc1qmekhqevphw53zglrnpf9p7jzmj9pajvtxgch0z, belongs to a cluster of addresses associated with an entity connected to RedVDS Defendants. **Figure 9** is a screenshot of the Chainalysis Reactor graph showing the on-chain tracing of the transaction to the RedVDS Defendants' BTC deposit address.

Fig. 9



13. Between April and November 2025, I conducted six separate purchases of infrastructure services from the RedVDS Defendants. On April 7, 2025, I acquired two instances of RedVDS infrastructure through the RedVDS website. Consistent with my prior test purchase, I accessed the platform, and made a payment via BTC, and I was issued receipts confirming the transactions, which included the following hashes: da9b06345500d3ba56fd58ac155c8d4bba1fff7709d452a645626188dddbb444 and

fd8b06300cf65008cfef27b35863cab77d054dfd063404909df8923a3cea4e36. See **Figure 10** and **Figure 11** below.

Fig. 10

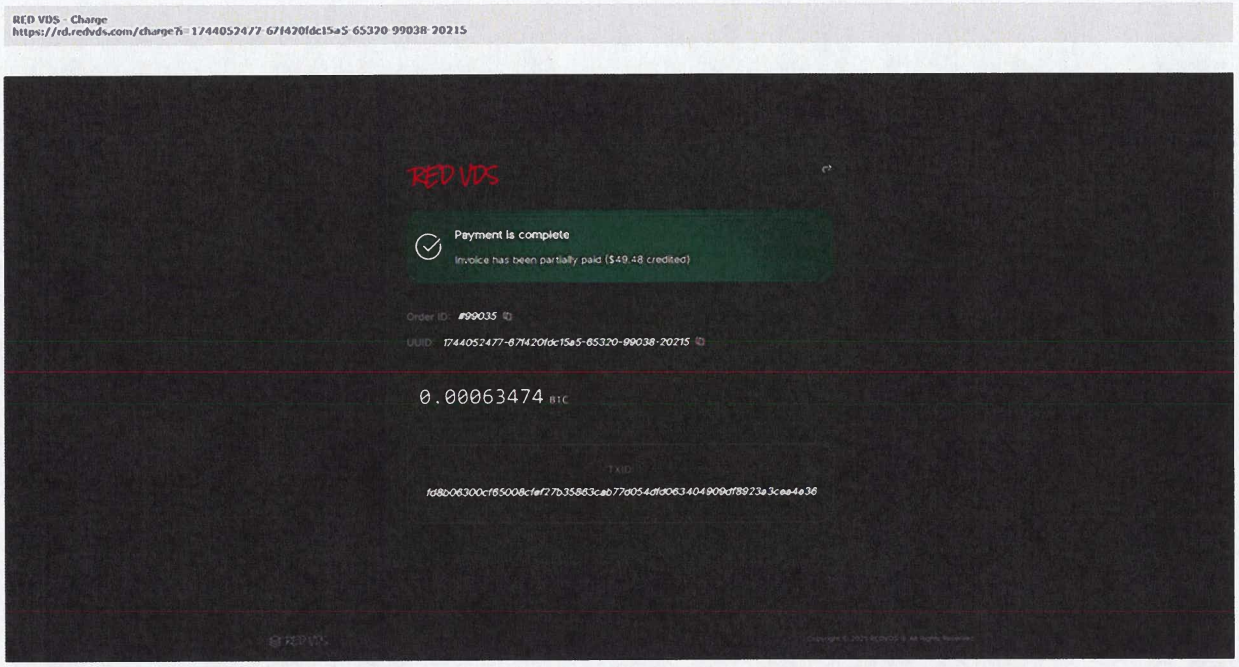
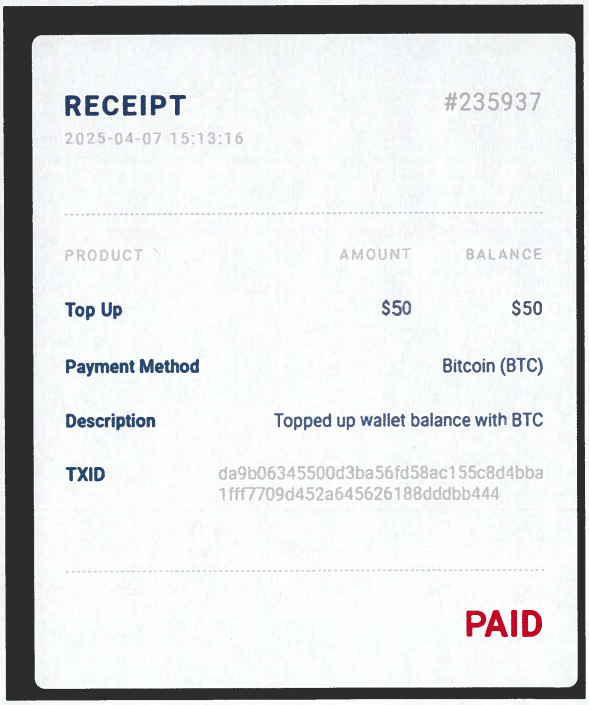
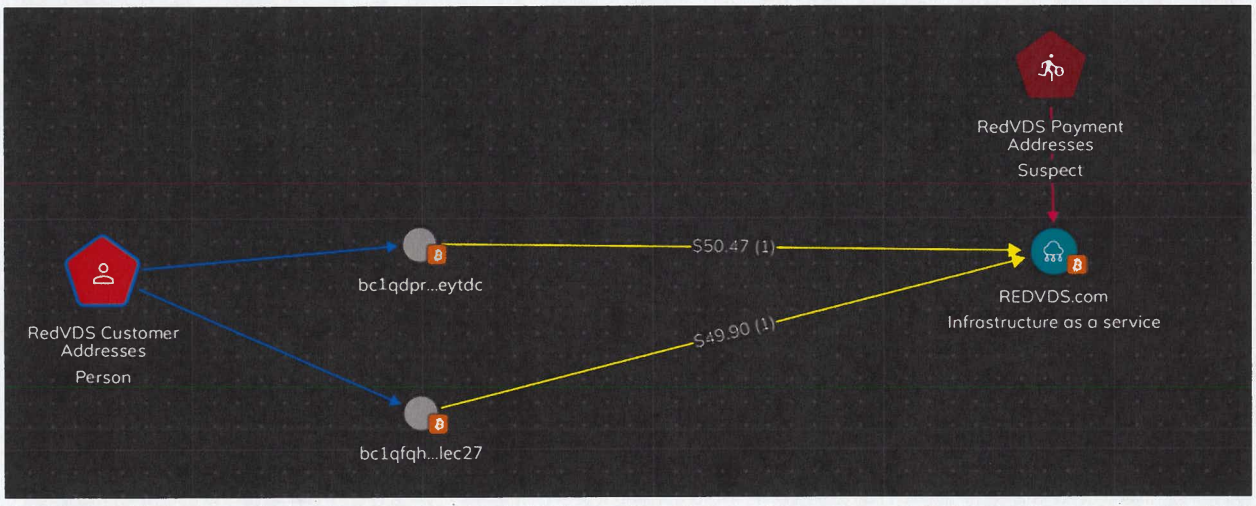


Fig. 11



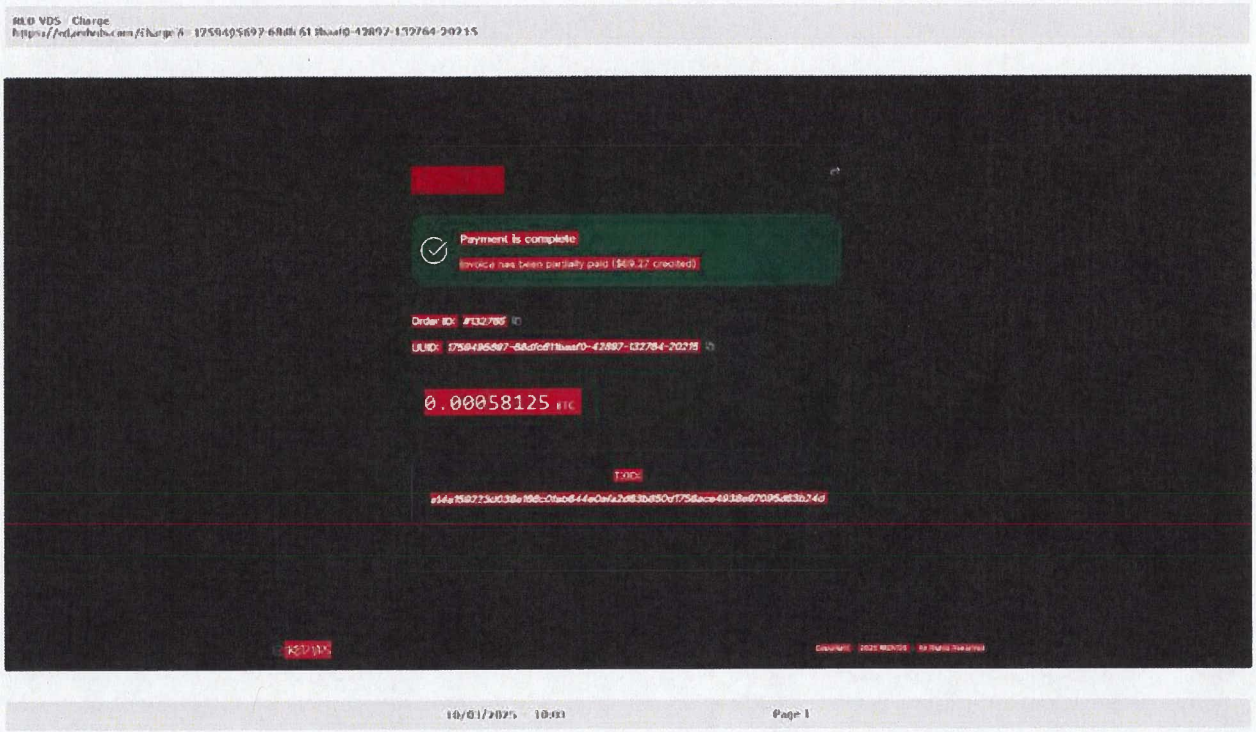
14. I conducted further analysis of both purchases using Chainalysis Reactor to examine the cryptocurrency transactions associated with the acquisition of RedVDS infrastructure. The investigation identified that the transaction hashes correspond to two distinct BTC addresses: bc1qmekhqevphw53zglrnpf9p7jzmj9pajvtxgch0z and bc1q9nynpus5c5jyhs3j3yz6yypmmgth9jd4tneqss. Both addresses are part of a previously identified BTC cluster linked to the RedVDS Defendants. **Figure 12** displays a screenshot from Chainalysis Reactor, illustrating the on-chain tracing of the transaction to the RedVDS Defendants' BTC addresses.

Fig. 12



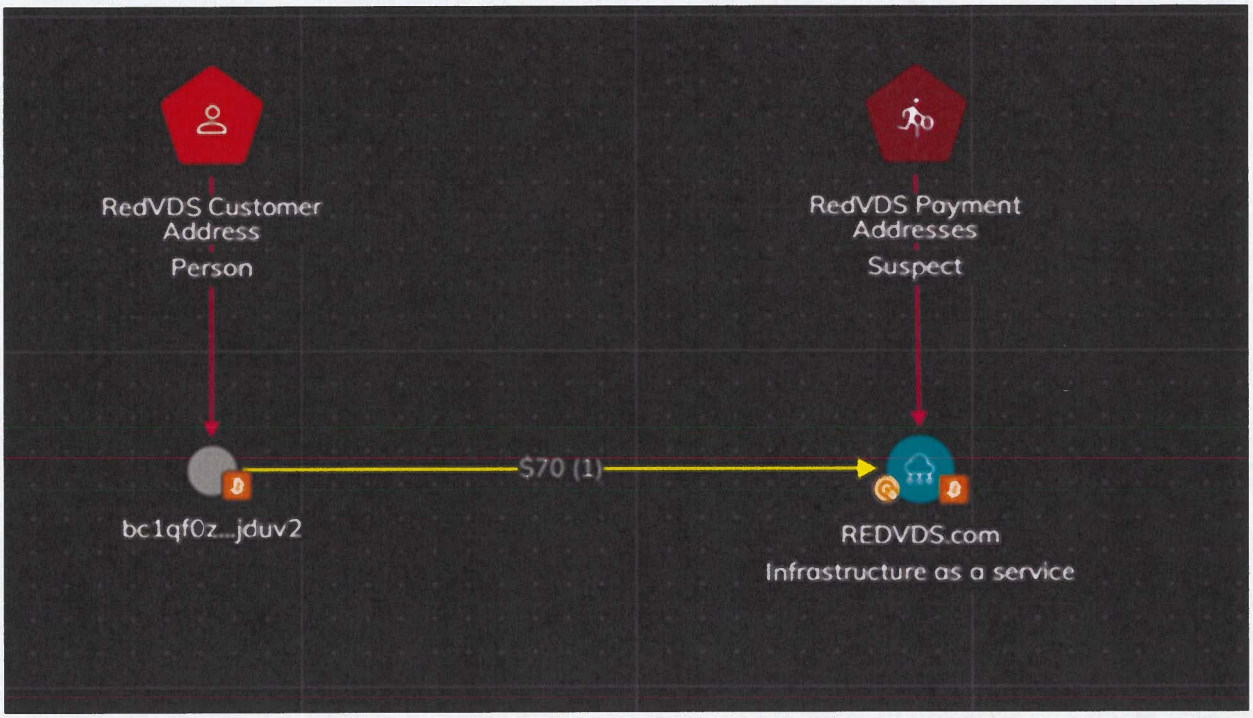
15. On October 3, 2025, DCU purchased a fourth instance of the RedVDS infrastructure through the RedVDS website. Like previous transactions, payment was made via BTC and DCU was issued a receipt confirming the transactions, which included the following hashes: a14e159223d038e166c0fab644e0afa2d63b850d1756ace4938e97095d63b24d. See **Figure 13** below.

Fig. 13



16. Using Chainalysis Reactor, DCU conducted blockchain analysis of transaction hash a14e159223d038e166c0fab644e0afa2d63b850d1756ace4938e97095d63b24d, which was linked to the purchase of a RedVDS server. Analysis indicated that the transaction was directed to BTC address bc1qxdxa50aycd98uk54j6wp054ftthe4ndjfup2zv, which belongs to the aforementioned cluster of addresses previously identified as being associated with the RedVDS website. **Figure 14** displays a screenshot from Chainalysis Reactor, illustrating the on-chain tracing of the transaction to the RedVDS Defendants' BTC addresses.

Fig. 14

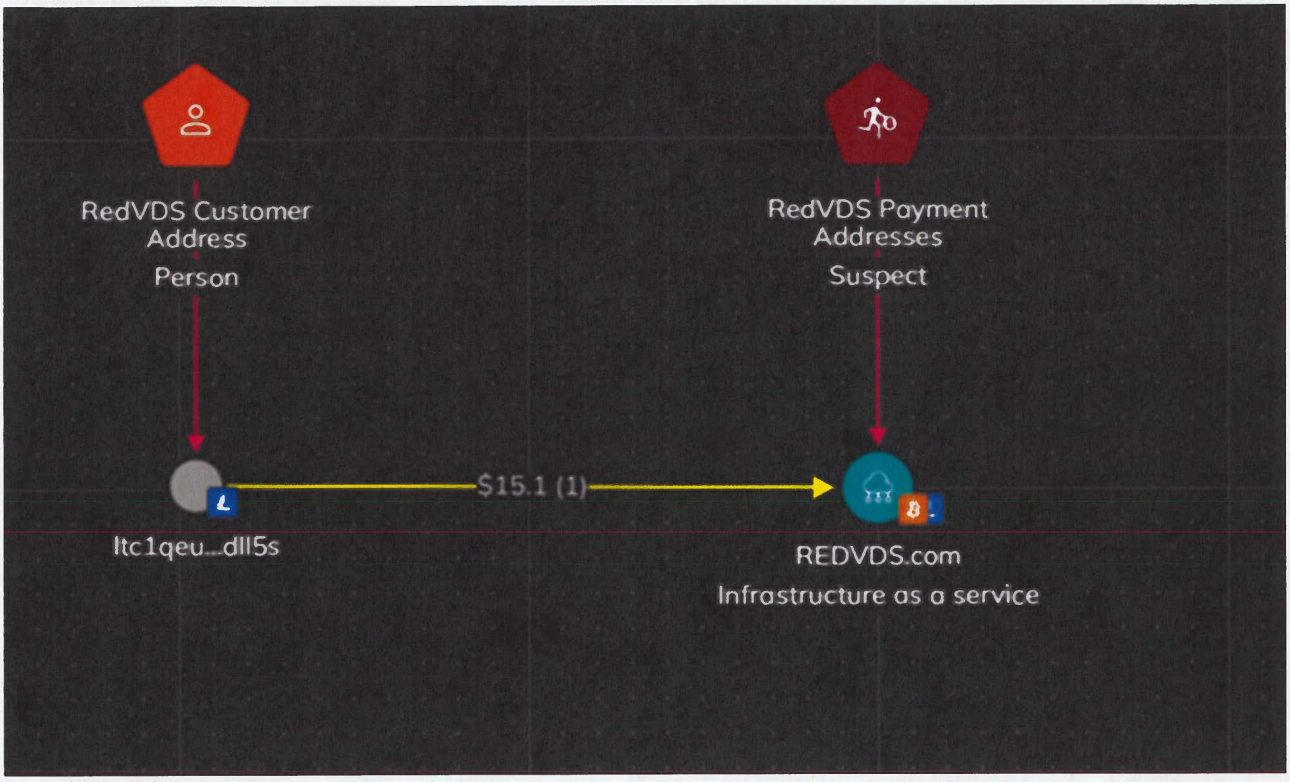


17. On October 31, 2025, DCU acquired a fifth instance of RedVDS infrastructure through the RedVDS website. As with my previous test purchases, DCU accessed the platform and completed the transaction this time using Litecoin (LTC), one of the various payment options offered by RedVDS. Upon completion, DCU received receipts confirming the transaction, which included the following transaction hash "8ab86e22c3ecbe89ef6bd544fdc6c660fdca698d1fdd8d1b27c4b79015d5f0fa". See **Figure 15** below.

Fig. 15

18. Using Chainalysis Reactor, I conducted on-chain analysis of transaction hash 8ab86e22c3ecbe89ef6bd544fdc6c660fdca698d1fdd8d1b27c4b79015d5f0fa, which was linked to the purchase of a RedVDS server. Analysis indicated that the transaction was directed to an LTC address, ltc1qhz530248kat0lsa289hg3h6l8t58q8r7sq5q92, which belongs to a cluster of addresses associated with an entity connected to RedVDS. **Figure 16** displays a screenshot from Chainalysis Reactor, illustrating the on-chain tracing of the transaction to the RedVDS Defendants' LTC addresses.

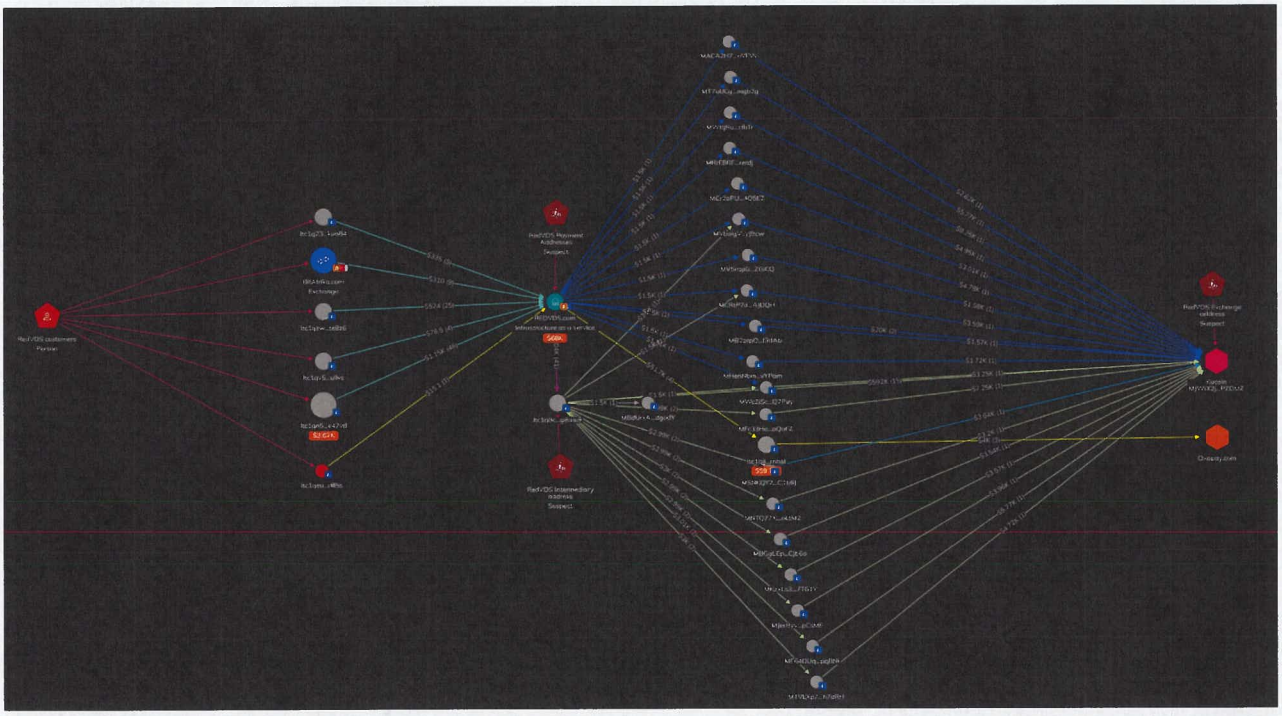
Fig. 16



RedVDS LTC on-chain analysis

19. Since its creation in January 2024, the cluster ltc1qhz530248kat0lsa289hg3h6l8t58q8r7sq5q92 has received approximately $425k USD in LTC as of December 18th, 2025. Subsequent analysis showed that roughly $417k USD in LTC was transferred from this cluster to a series of intermediary addresses, including LTC address ltc1q8crk2fclxj8y984574ncwaukcagedzq2pg8am9, which appears to have received most of the funds. These intermediary addresses then transferred the majority of funds to an LTC address hosted on the cryptocurrency exchange Kucoin.com that has been active since June 2023. Further on-chain transaction analysis identified that some funds were sent to a merchant service called Oxapay.com. **Figure 17** displays a screenshot from Chainalysis Reactor, illustrating the on-chain tracing of the transactional flow from the RedVDS LTC Cluster.

Fig. 17



20. On November 18–19, 2025, I acquired a sixth and seventh instance of RedVDS infrastructure through the RedVDS website. Like previous transactions, payment was made via BTC and I was issued a receipt confirming the transactions, which included the following hashes: f899f82cbb7a09dd3777e464c81213203e1af7447e93bc995a9c6e0e7c9151a8 and 98b923b1c0b7294a7dd22e74352e6feaf38060f040f5bb241bfa1c898b54ddad. See **Figure 18** and **Figure 19** below.

Fig. 18

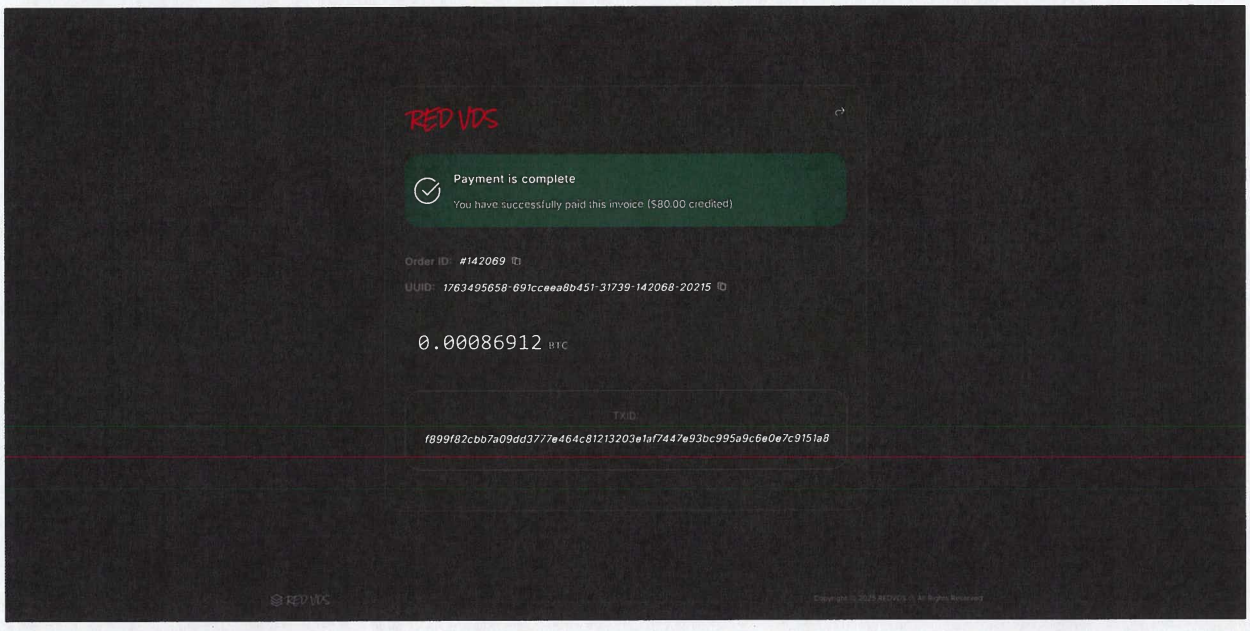
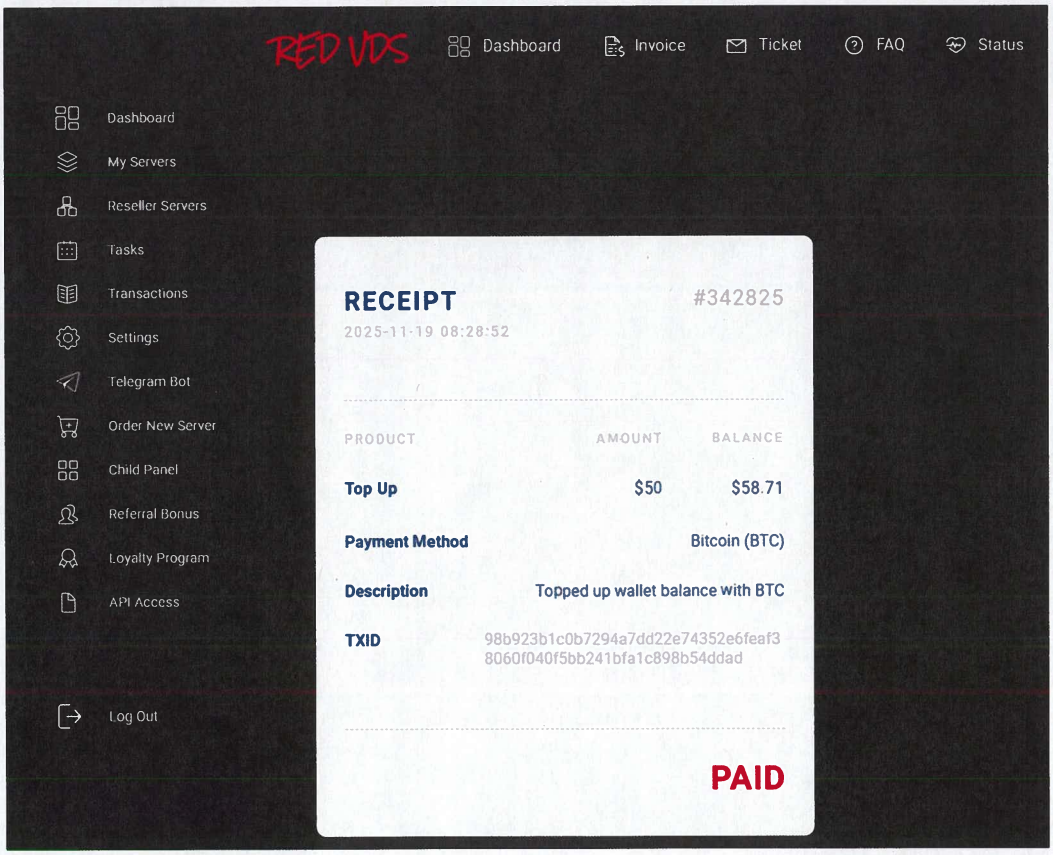
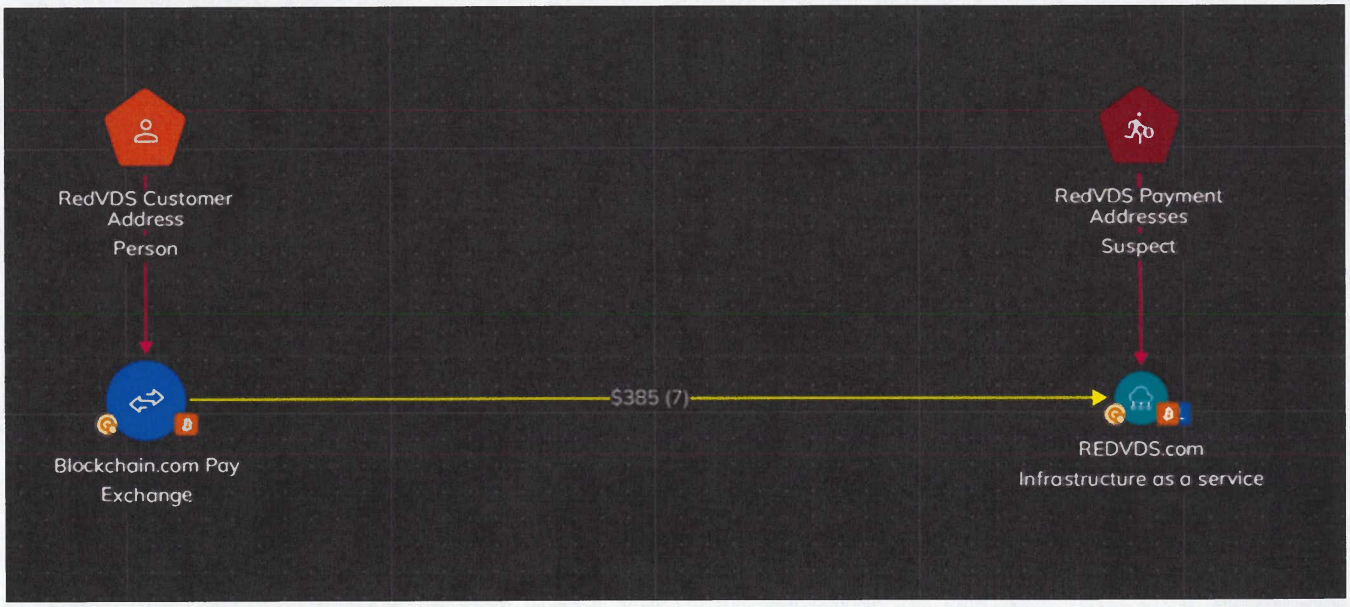

RED VDS
Payment is complete
You have successfully paid this invoice ($80.00 credited)
Order ID: #142069
UUID: 1763495658-691cceea8b451-31739-142068-20215
0.00086912 BTC
TXID
f899f82cbb7a09dd3777e464c81213203e1af7447e93bc995a9c6e0e7c9151a8

Fig. 19


RED VDS
Dashboard
Invoice
Ticket
FAQ
Status
Dashboard
My Servers
Reseller Servers
Tasks
Transactions
Settings
Telegram Bot
Order New Server
Child Panel
Referral Bonus
Loyalty Program
API Access
Log Out
RECEIPT
#342825
2025-11-19 08:28:52
PRODUCT
AMOUNT
BALANCE
Top Up
$50
$58.71
Payment Method
Bitcoin (BTC)
Description
Topped up wallet balance with BTC
TXID
98b923b1c0b7294a7dd22e74352e6feaf3
8060f040f5bb241bfa1c898b54ddad
PAID

21. Using Chainalysis Reactor, I conducted blockchain analysis of transaction hashes f899f82cbb7a09dd3777e464c81213203e1af7447e93bc995a9c6e0e7c9151a8 and 98b923b1c0b7294a7dd22e74352e6feaf38060f040f5bb241bfa1c898b54ddad, which was linked to the purchase of a RedVDS server. Analysis indicated that the transactions were directed to BTC address bc1qxdxa50aycd98uk54j6wp054ftthe4ndjfup2zv, which belongs to the aforementioned cluster of addresses previously identified as being associated with the RedVDS website. Since its creation in May 2024, this cluster has received approximately $2MM USD in BTC to date. **Figure 20** displays a screenshot from Chainalysis Reactor, illustrating the on-chain tracing of the transaction to the RedVDS Defendants' BTC addresses.

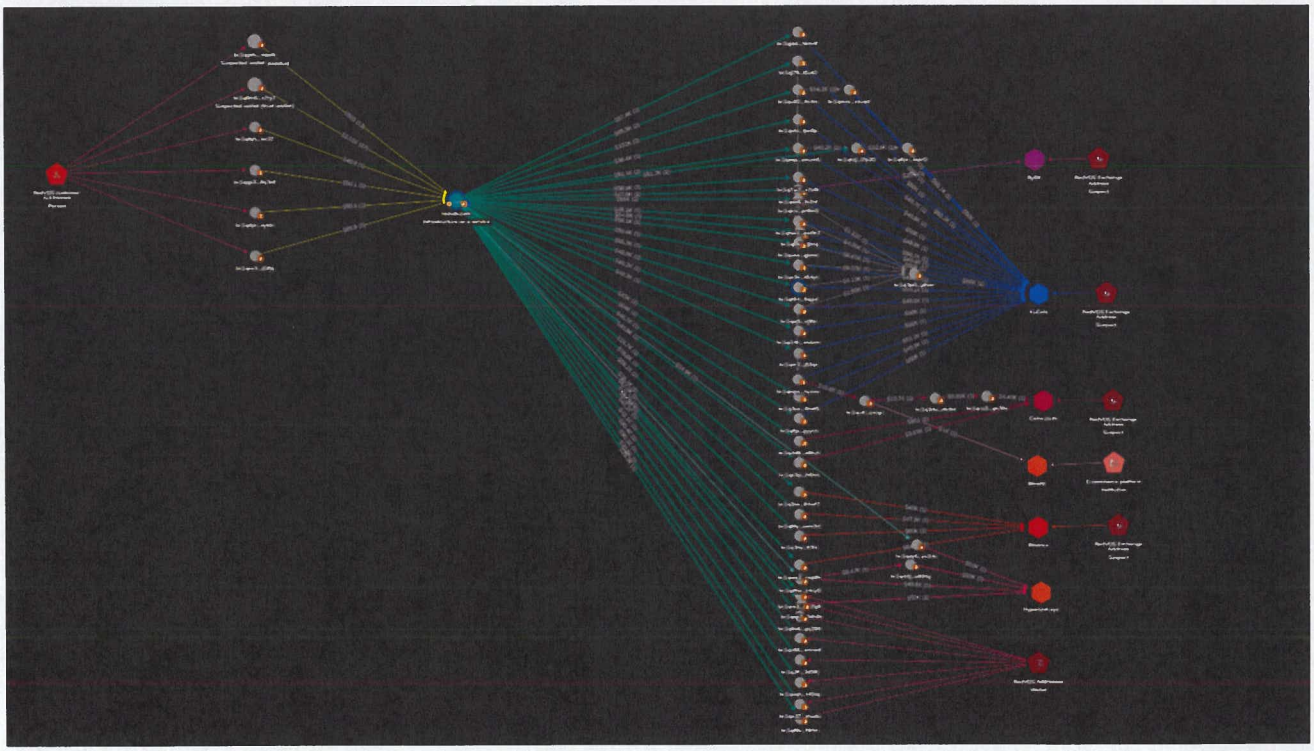
Fig. 20



RedVDS BTC on-chain analysis

22. Using Chainalysis Reactor, I investigated the on-chain transactional flow of funds that have been sent from the aforementioned BTC cluster associated with the entity RedVDS. The analysis revealed that approximately $2MM USD in BTC was transferred from this cluster to a series of intermediary addresses, which subsequently transferred the funds to BTC addresses hosted on cryptocurrency exchanges Binance, Bybit, Bitrefill, Kucoin.com and Coins.co.th. Additional analysis identified that some funds were sent to hyperunit.xyz a decentralized exchange (DEX) that is used for chain swapping. Cumulative analysis determined that the total amount of funds sent through these intermediary addresses to the aforementioned exchanges amounted to approximately $4.3MM USD in BTC as of December 18th, 2025. A Chainalysis graph illustrating the on-chain transaction flow from the RedVDS BTC cluster addresses is provided below in **Figure 21**.

Fig. 21



23. In total, I have been able to trace since June 2023, at least $5.3MM in cryptocurrency transactions that have been linked to purchases of the RedVDS Enterprise. This amount likely represents only a portion of the total revenue, as our analysis is limited to the cryptocurrencies used during the controlled purchases. RedVDS accepted payments in additional cryptocurrencies that were not included in our purchases.

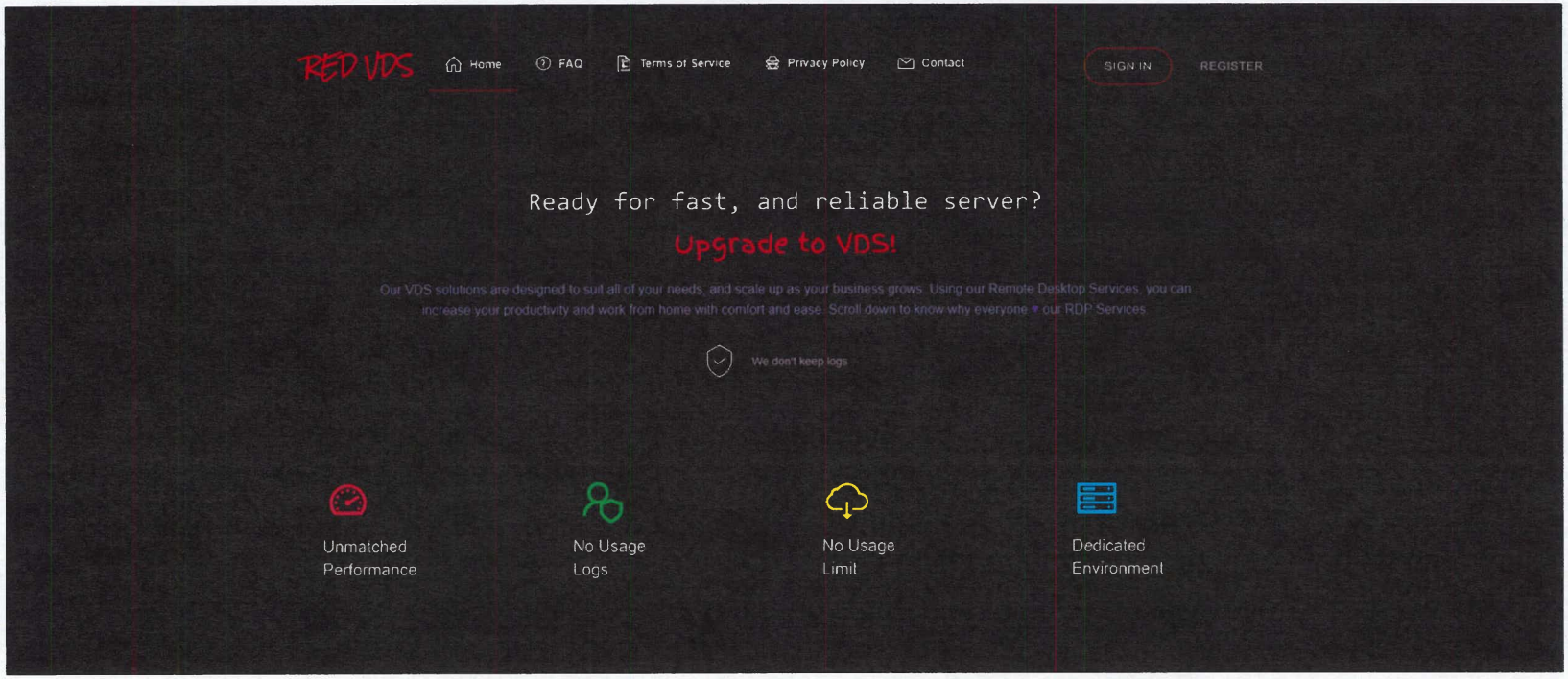
24. Not only did the test purchases allow me to trace the financial transactions and uncover operational details, it also provided Microsoft with information about how the RedVDS Enterprise works, how they can be used by cybercriminals, and how stolen credentials are delivered.

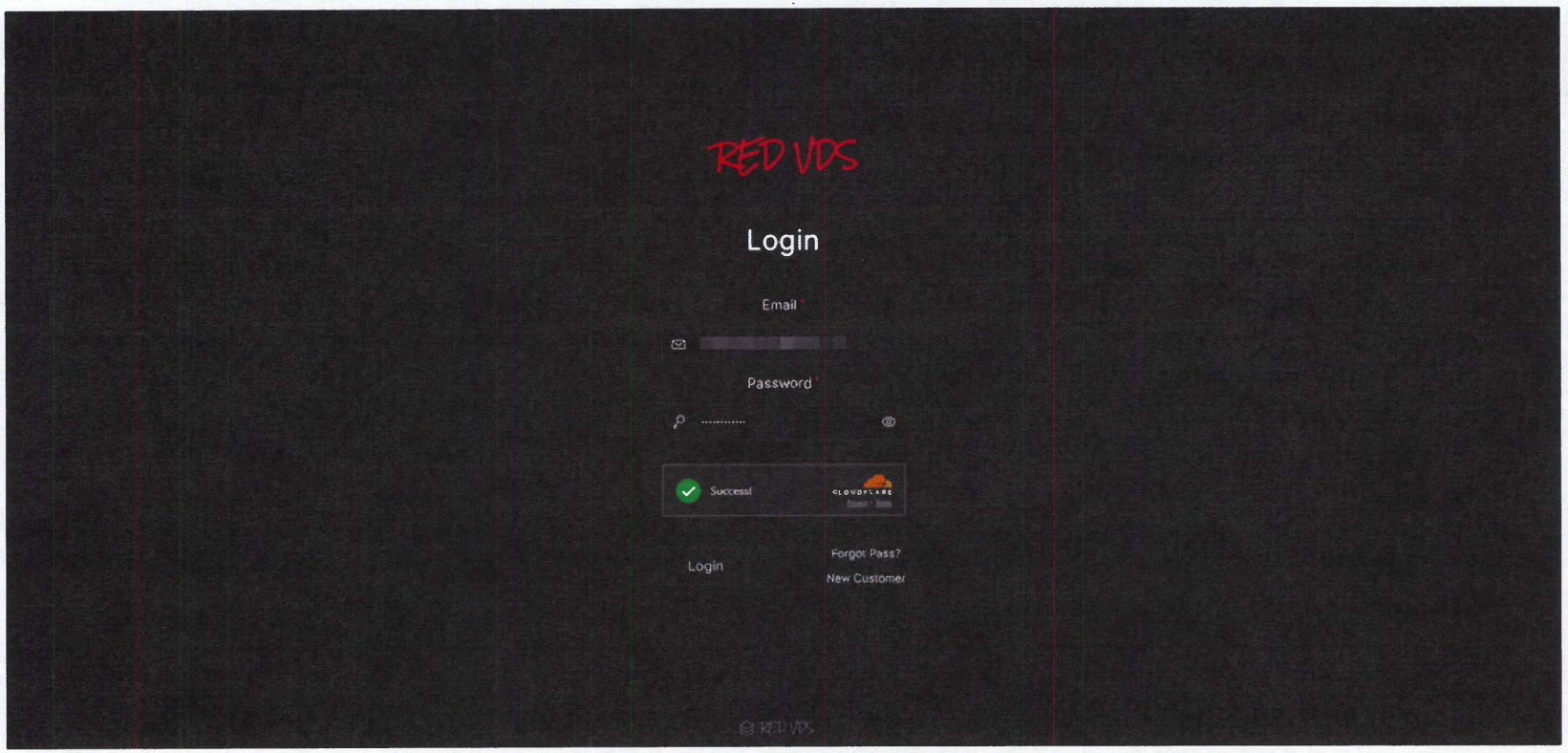
25. Attached to this declaration as Exhibit 1 is a true and correct compilation of screen shots I took of the RedVDS user interface during the test buy process described above. Certain information has been obfuscated from some of these screen captures for operational security purposes.

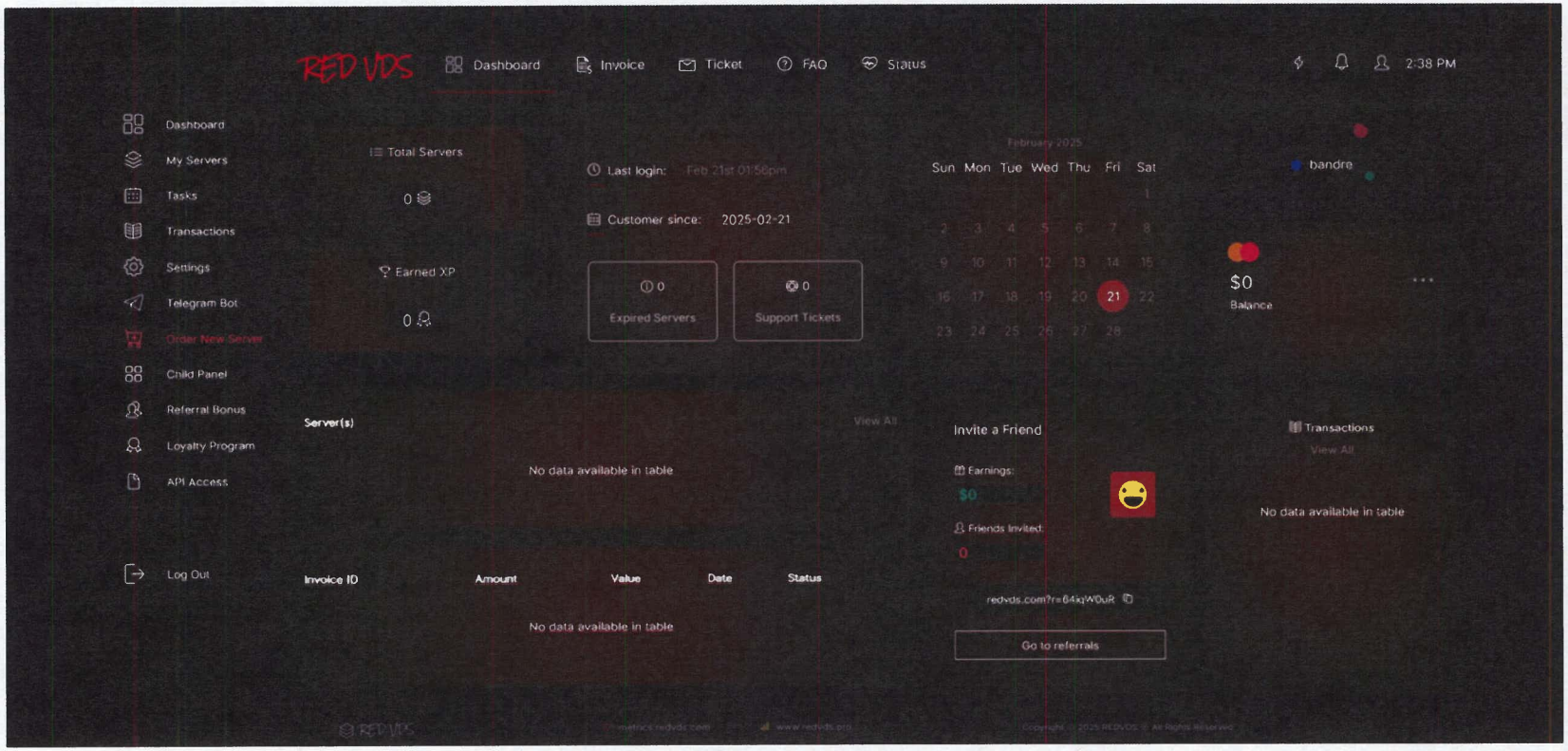
I declare under penalty of perjury under the laws of the United States that the forgoing is true and correct to the best of my knowledge. Executed this 6th day of January, 2026 at Miami, Florida.

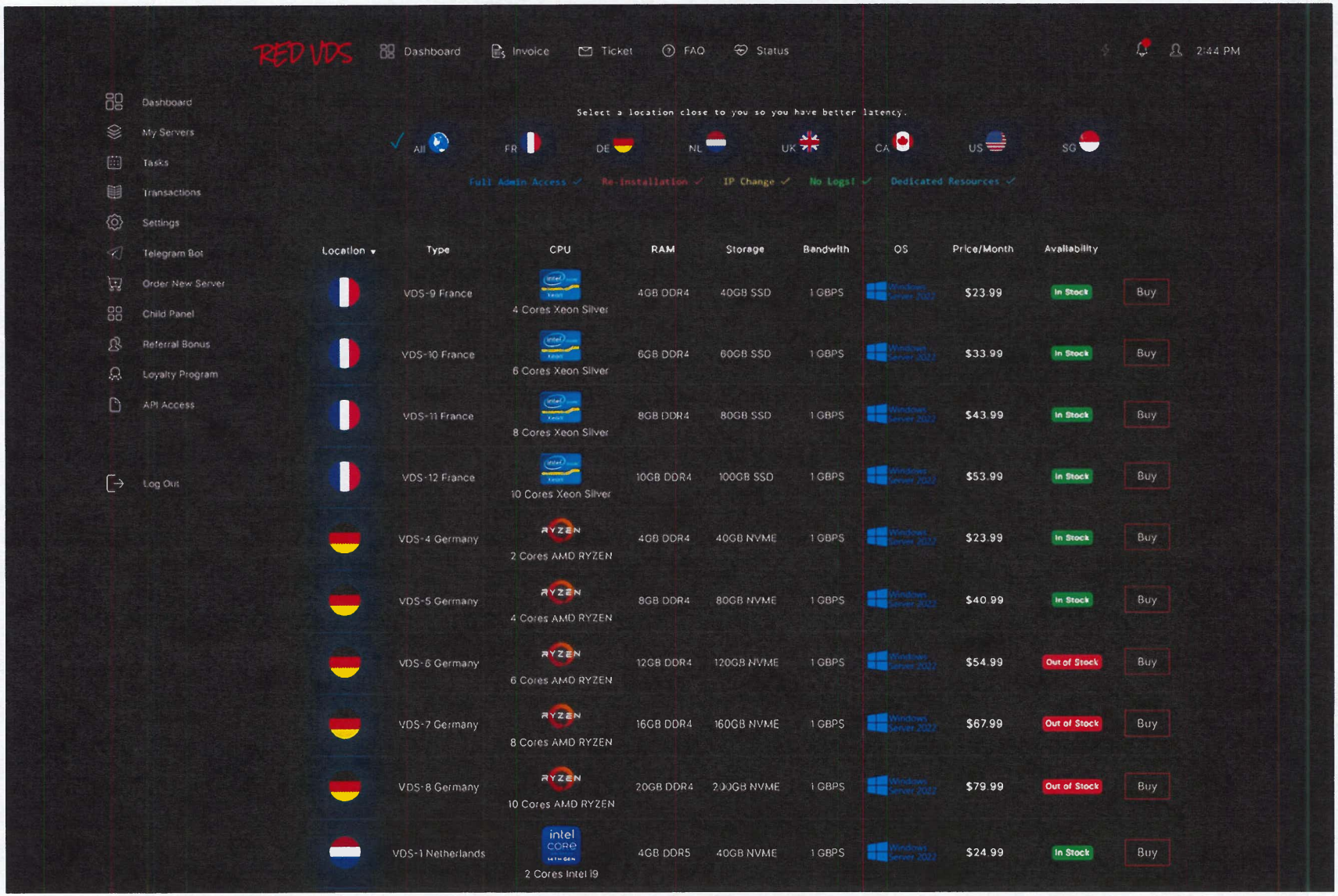
Maurice Mason

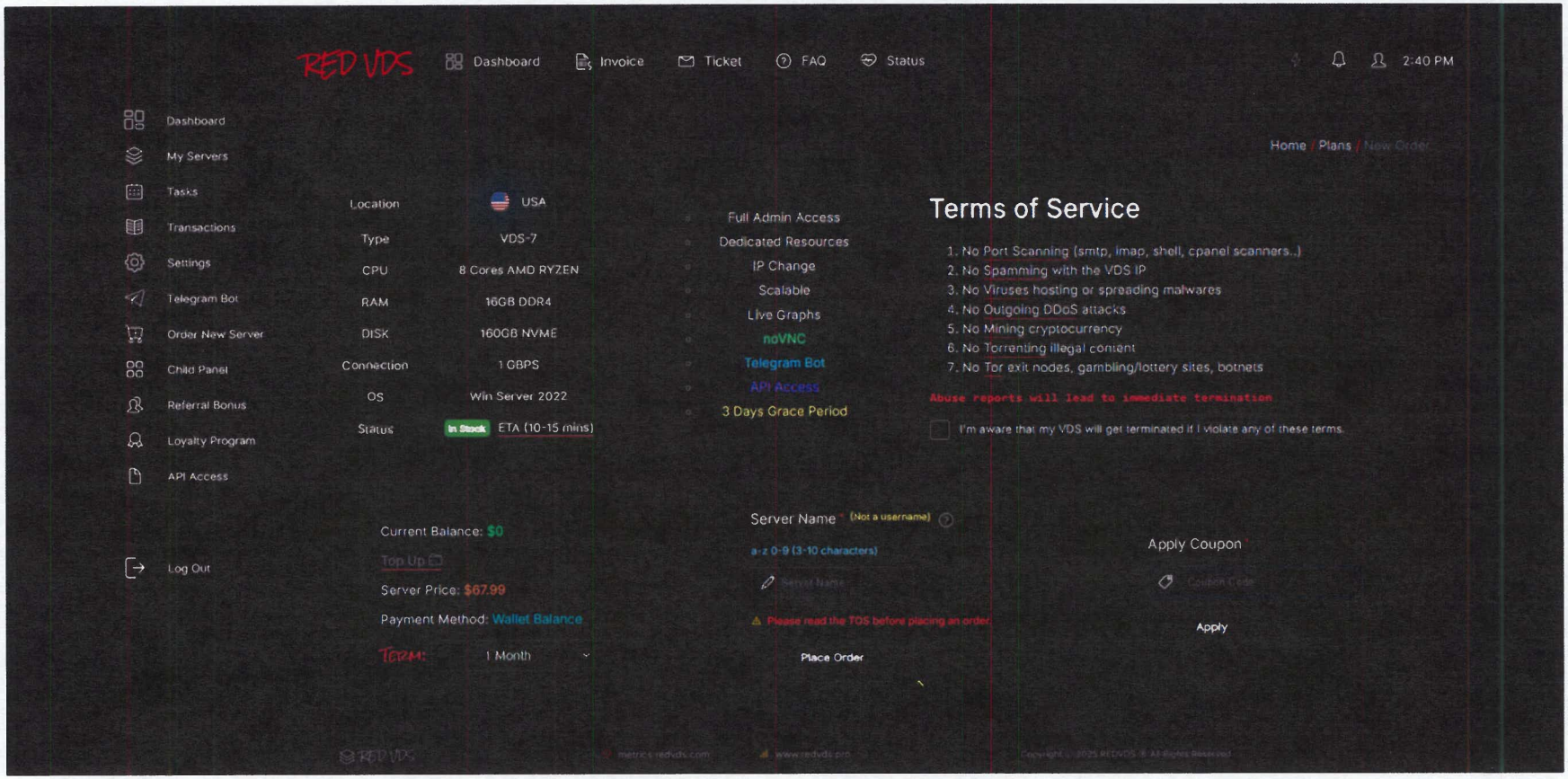
Exhibit 1


RED VDS
Home
FAQ
Terms of Service
Privacy Policy
Contact
SIGN IN
REGISTER
Ready for fast, and reliable server?
Upgrade to VDS!
Our VDS solutions are designed to suit all of your needs, and scale up as your business grows. Using our Remote Desktop Services, you can increase your productivity and work from home with comfort and ease. Scroll down to know why everyone ♥ our RDP Services
We don't keep logs
Unmatched Performance
No Usage Logs
No Usage Limit
Dedicated Environment


RED VDS
Login
Email *
Password *
Success!
CLOUDFLARE
Login
Forgot Pass?
New Customer
RED VDS


RED VDS
Dashboard
Invoice
Ticket
FAQ
Status
2:38 PM
Dashboard
My Servers
Tasks
Transactions
Settings
Telegram Bot
Order New Server
Child Panel
Referral Bonus
Loyalty Program
API Access
Log Out
Total Servers
0
Earned XP
0
Last login: Feb 21st 01:58pm
Customer since: 2025-02-21
0
Expired Servers
0
Support Tickets
February 2025
Sun Mon Tue Wed Thu Fri Sat
1
2 3 4 5 6 7 8
9 10 11 12 13 14 15
16 17 18 19 20 21 22
23 24 25 26 27 28
bandre
$0
Balance
Server(s)
View All
No data available in table
Invite a Friend
Earnings:
$0
Friends Invited:
0
redvds.com?r=64xjWDuR
Go to referrals
Transactions
View All
No data available in table
Invoice ID
Amount
Value
Date
Status
No data available in table


RED VDS
Dashboard
Invoice
Ticket
FAQ
Status
2:44 PM
Dashboard
My Servers
Tasks
Transactions
Settings
Telegram Bot
Order New Server
Child Panel
Referral Bonus
Loyalty Program
API Access
Log Out
Select a location close to you so you have better latency.
All
FR
DE
NL
UK
CA
US
SG
Full Admin Access ✓
Re-installation ✓
IP Change ✓
No Logs! ✓
Dedicated Resources ✓
Location
Type
CPU
RAM
Storage
Bandwith
OS
Price/Month
Availability
VDS-9 France
4 Cores Xeon Silver
4GB DDR4
40GB SSD
1 GBPS
$23.99
In Stock
Buy
VDS-10 France
6 Cores Xeon Silver
6GB DDR4
60GB SSD
1 GBPS
$33.99
In Stock
Buy
VDS-11 France
8 Cores Xeon Silver
8GB DDR4
80GB SSD
1 GBPS
$43.99
In Stock
Buy
VDS-12 France
10 Cores Xeon Silver
10GB DDR4
100GB SSD
1 GBPS
$53.99
In Stock
Buy
VDS-4 Germany
2 Cores AMD RYZEN
4GB DDR4
40GB NVME
1 GBPS
$23.99
In Stock
Buy
VDS-5 Germany
4 Cores AMD RYZEN
8GB DDR4
80GB NVME
1 GBPS
$40.99
In Stock
Buy
VDS-6 Germany
6 Cores AMD RYZEN
12GB DDR4
120GB NVME
1 GBPS
$54.99
Out of Stock
Buy
VDS-7 Germany
8 Cores AMD RYZEN
16GB DDR4
160GB NVME
1 GBPS
$67.99
Out of Stock
Buy
VDS-8 Germany
10 Cores AMD RYZEN
20GB DDR4
200GB NVME
1 GBPS
$79.99
Out of Stock
Buy
VDS-1 Netherlands
2 Cores Intel i9
4GB DDR5
40GB NVME
1 GBPS
$24.99
In Stock
Buy


RED VDS
Dashboard
Invoice
Ticket
FAQ
Status
2:40 PM
Dashboard
My Servers
Tasks
Transactions
Settings
Telegram Bot
Order New Server
Child Panel
Referral Bonus
Loyalty Program
API Access
Log Out
Home / Plans / New Order
Location
USA
Type
VDS-7
CPU
8 Cores AMD RYZEN
RAM
16GB DDR4
DISK
160GB NVME
Connection
1 GBPS
OS
Win Server 2022
Status
In Stock
ETA (10-15 mins)
Full Admin Access
Dedicated Resources
IP Change
Scalable
Live Graphs
noVNC
Telegram Bot
API Access
3 Days Grace Period
Terms of Service
1. No Port Scanning (smtp, imap, shell, cpanel scanners..)
2. No Spamming with the VDS IP
3. No Viruses hosting or spreading malwares
4. No Outgoing DDoS attacks
5. No Mining cryptocurrency
6. No Torrenting illegal content
7. No Tor exit nodes, gambling/lottery sites, botnets
Abuse reports will lead to immediate termination
I'm aware that my VDS will get terminated if I violate any of these terms.
Current Balance: $0
Top Up
Server Price: $67.99
Payment Method: Wallet Balance
TERM:
1 Month
Server Name * (Not a username)
a-z 0-9 (3-10 characters)
Please read the TOS before placing an order.
Place Order
Apply Coupon
Apply

RED VDS

To make a payment, send BTC by scanning the QR code or copy the address below.

Order ID

#91038

Bitcoin Address

bc1qmekhqevphw53zglrnpf9p7jzmj9pajvtxgch0z

Amount

0.00072014

Value

$68 USD 5% cashback on $250+ top ups

Open in Wallet

59:54 Time left

Status Waiting For Payment

Last Checked -

[We require 1 confirmation for BTC transactions]

This is a static wallet

Transaction Fees

Fast: 3 sat/vB [10 min]

Normal: 3 sat/vB [30 min]

Slow: 3 sat/vB [60 min]

RED VDS

RED VDS

Dear [redacted]

Your invoice 91038 has been paid successfully. Detailed information can be found below.

Received Amount: 0.00073385
Payment Method: BTC
Type: Top Up

- RED VDS