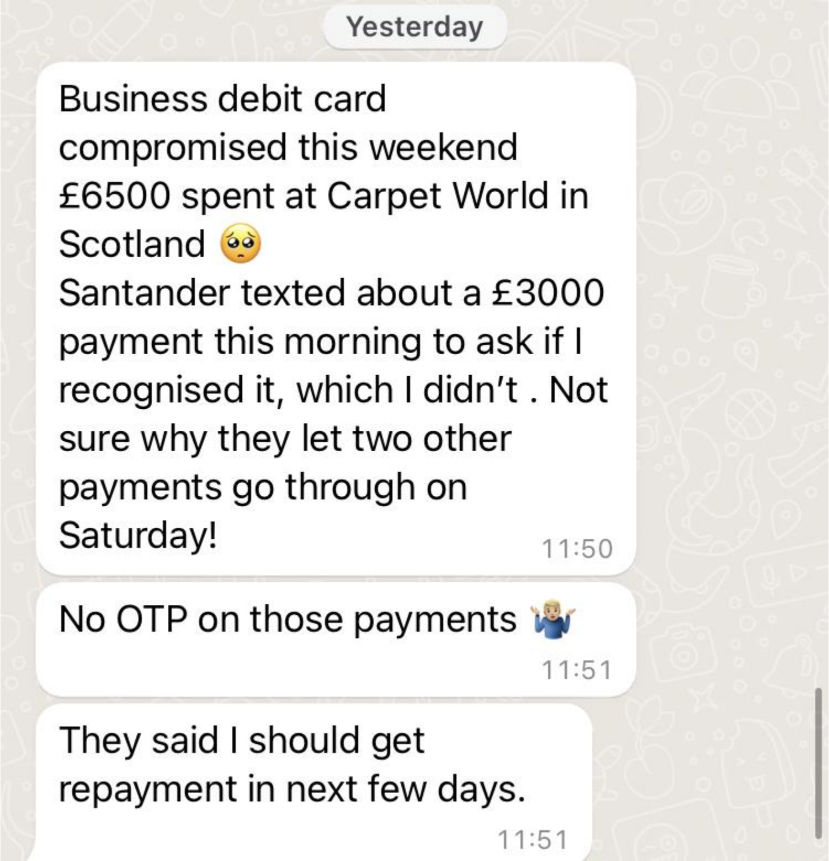
Carding: The Global Epidemic

Bushido | Bournemouth 2600

Case Study: Local Retailer 1 (LR1)

- LR1 is a family-owned retailer in Bournemouth
- LR1 had a business debit card compromised
- The incident happened on a Saturday morning
- £6,500 charged at Carpet World (in Scotland)
- Another £3,000 attempted charge
- Santander bank texted about payment auth for the 3rd transaction, but let the other two through
- LR1 didn’t receive a one-time passcode (OTP) requested to authorize the debit card charges



Yesterday

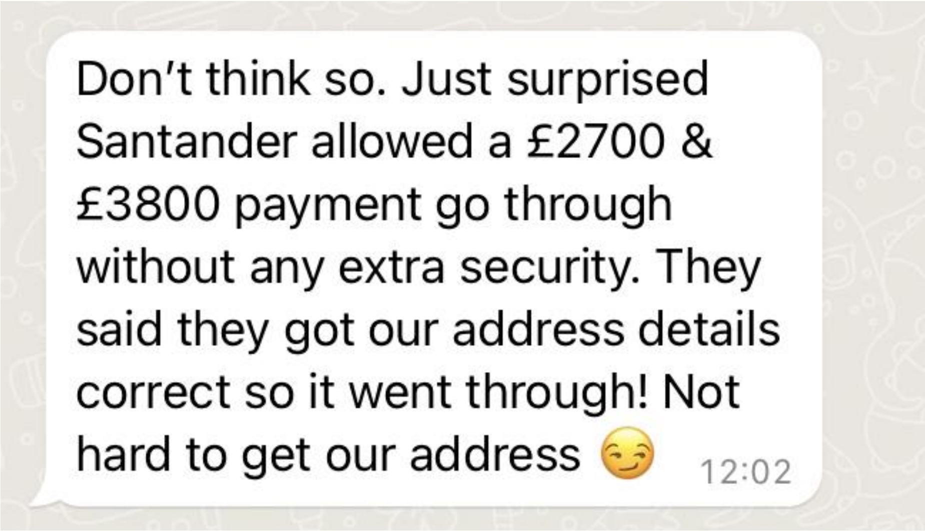
Business debit card compromised this weekend £6500 spent at Carpet World in Scotland 🥺
Santander texted about a £3000 payment this morning to ask if I recognised it, which I didn't . Not sure why they let two other payments go through on Saturday! 11:50

No OTP on those payments 🤷🏼‍♂️ 11:51

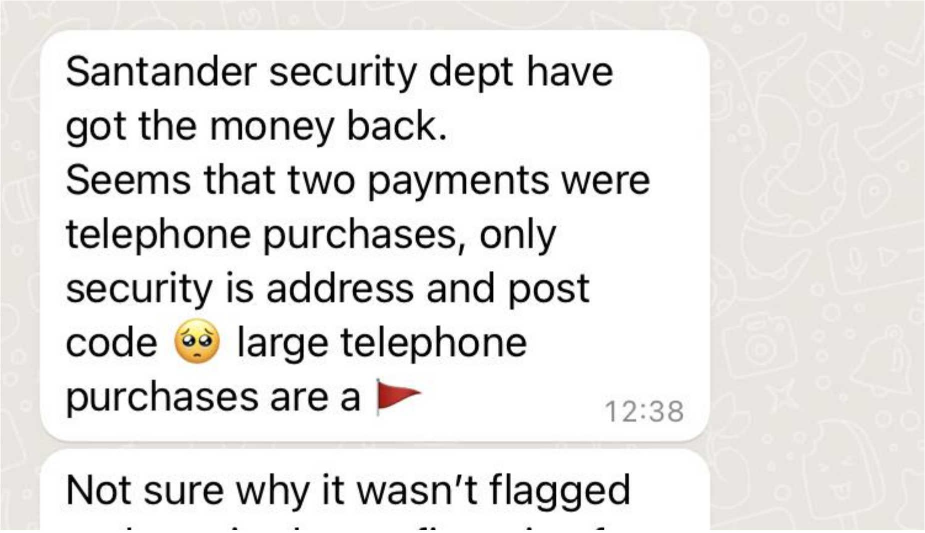
They said I should get repayment in next few days. 11:51

Case Study: LR1 (Continued)

- Santander Counter-Fraud began to investigate
- The three unauthorized card charges were initiated via telephone card-not-present purchases
- The first one was £2,700 and the second was £3,800, the last was £3,000
- The only bit of information required to verify and permit the charges is the local retailer’s public address
- No in-app notifications or text messages were sent to the local retailer



Don’t think so. Just surprised Santander allowed a £2700 & £3800 payment go through without any extra security. They said they got our address details correct so it went through! Not hard to get our address 😏 12:02

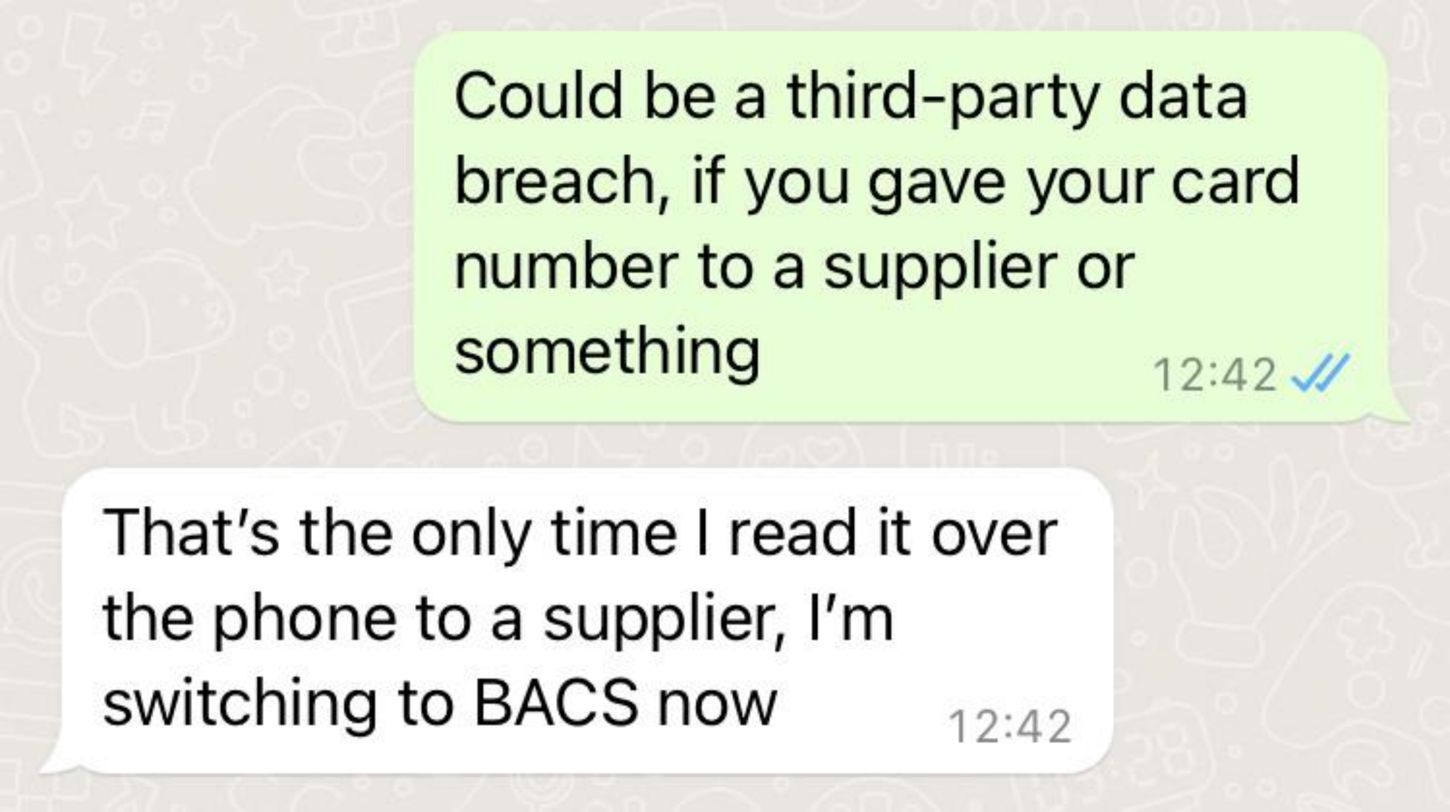


Santander security dept have got the money back.
Seems that two payments were telephone purchases, only security is address and post code 🥺 large telephone purchases are a 🚩 12:38

Not sure why it wasn’t flagged

Potential source of the LR1 debit card breach

- The debit card is rarely used, normally the bank account is used for Bankers' Automated Clearing System (BACS) transfers
- The retailer did realise, however, that they read the whole 16-digit, plus expiry, plus 3-digit CVV over the phone for a supplier

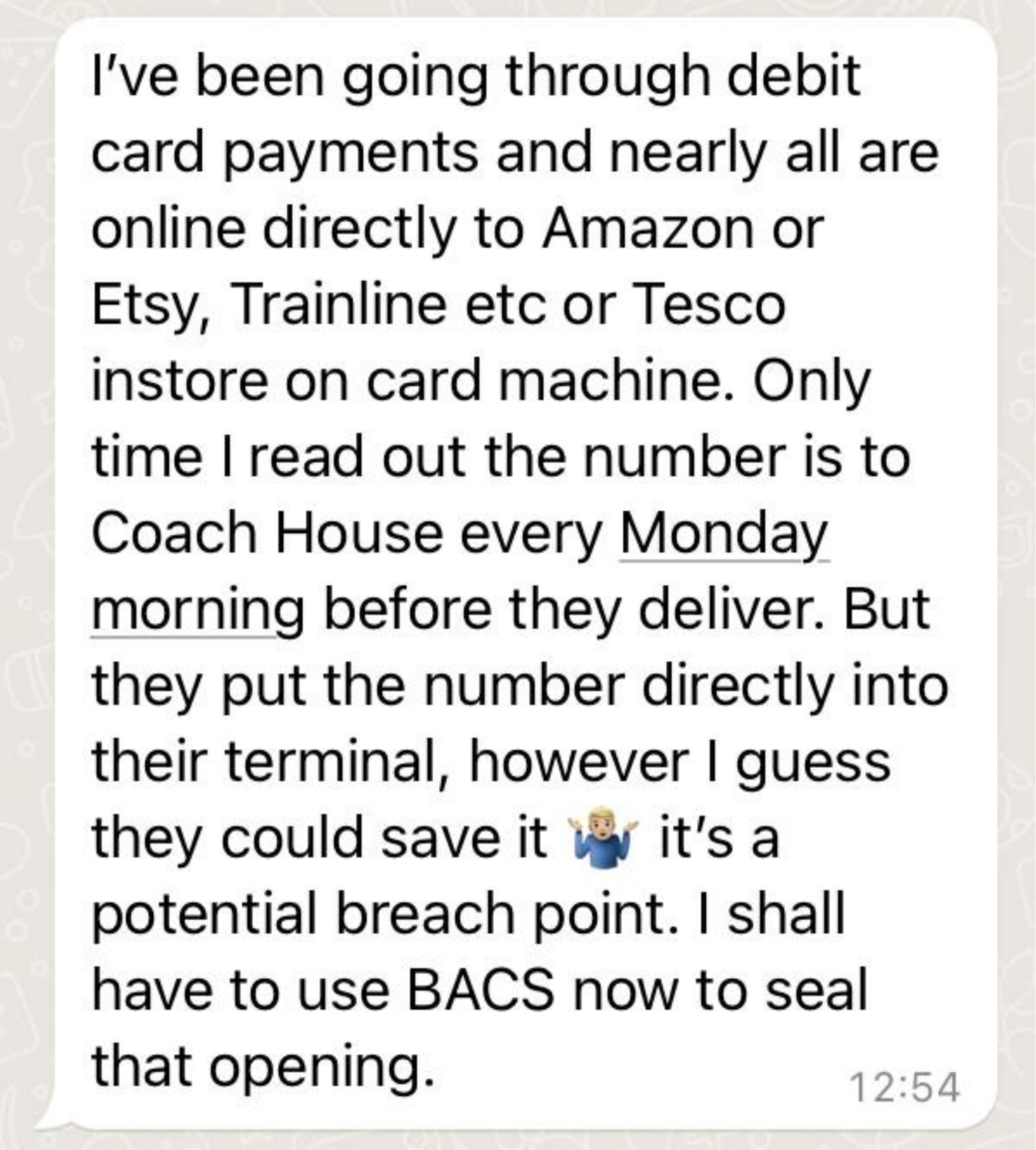


Could be a third-party data breach, if you gave your card number to a supplier or something 12:42 ✓✓

That's the only time I read it over the phone to a supplier, I'm switching to BACS now 12:42

Triaging LR1's payment history

- I triaged LR1's history through the compromised debit card's payments which were mostly to Amazon, Etsy, Trainline, and Tesco
- The only time when the full card number is given out is to 'Coachhouse.com' a furniture manufacturer, which was over the phone (card-not-present payments) for their supplies
- The likelihood of them being compromised versus Amazon, Etsy, Trainline or Tesco is much higher



I've been going through debit card payments and nearly all are online directly to Amazon or Etsy, Trainline etc or Tesco instore on card machine. Only time I read out the number is to Coach House every Monday morning before they deliver. But they put the number directly into their terminal, however I guess they could save it 🤷🏼‍♂️ it's a potential breach point. I shall have to use BACS now to seal that opening. 12:54

LR1’s Remediation

- **First** – Santander refunded the victim the stolen money
- **Second** – The card was cancelled a new one was sent
- **Third** – Telephone card-not-present purchases have been disabled, only BACS transfers are used to pay suppliers
- **Fourth** – Any charges over £100 require biometric verification

Best Practices for LR1

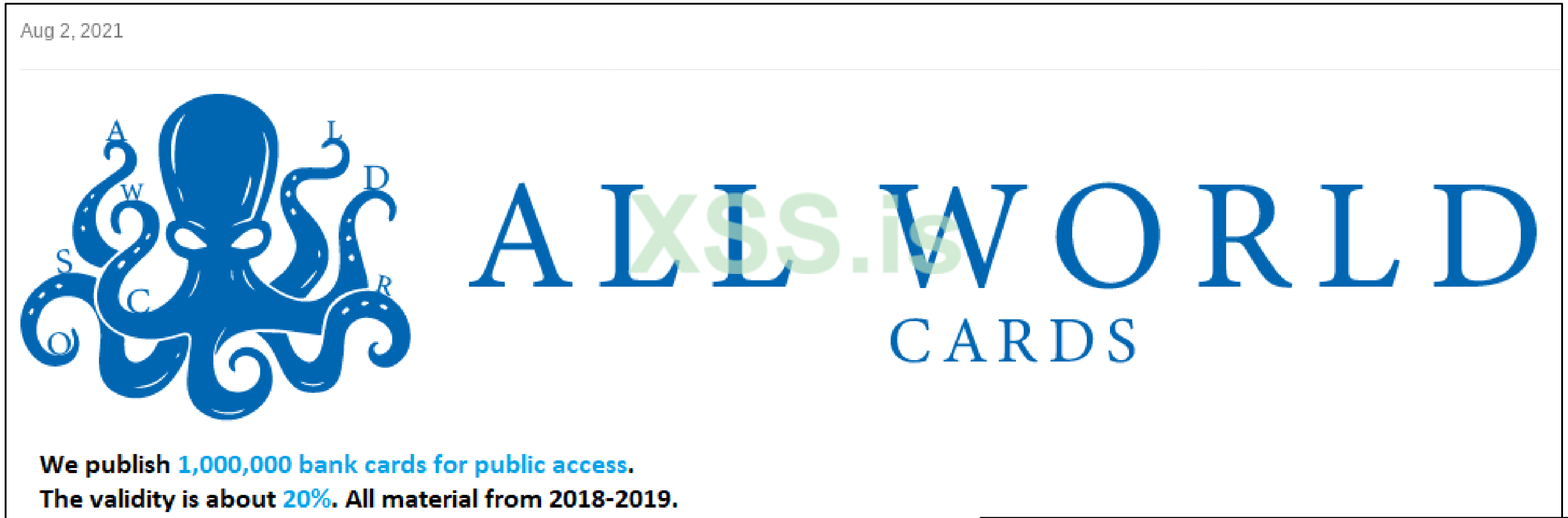
- **First** – regularly monitor bank statements for any abnormal charges
- **Second** – be mindful of giving out the card number, especially all three codes (16-digit, expiry, and CVV) to a supplier
- **Third** – keep the physical card number protected, either on your person or in a locked safe
- **Fourth** – use secure networks when entering the card number, be mindful of sites with SSL/TLS certificates or public WiFi
- **Fifth** – be mindful of phishing attacks, SMS Phishing and Automated Voice Phishing is common
- **Sixth** – If a customer on the phone is going to pick up the goods anyways, the shop owner should have insisted that the customer pay for the goods in-store, using the normal chip & PIN method.

Card-Not-Present (CNP) Fraud

- To commit CNP fraud, a cybercriminal needs to obtain the following information:
- Card number
- Cardholder name
- Billing address
- 3-digit CVV/CVC security code
- Card expiration date

- **Stats around CNP Fraud from Thales**
- CNP fraud was estimated at $4.5 billion for 2016 by the US federal reserve in a 2018 report
- In the EU, CNP payments counted for a massive 79% of the total value of card fraud for 2018
- In the UK, CNP is 76% of the total value of card fraud in 2019
- In 2017, CNP fraud in Australia accounted for 85% of all fraud

The Carding Markets



Aug 2, 2021

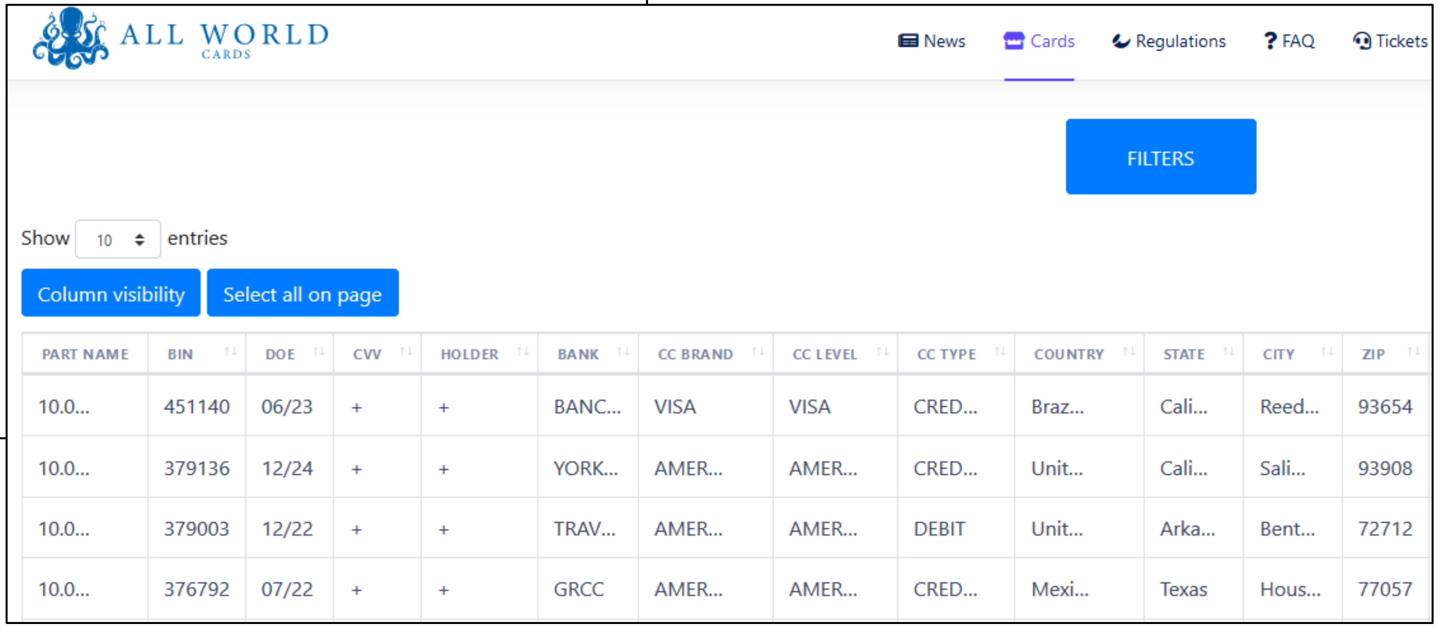
We publish 1,000,000 bank cards for public access.
The validity is about 20%. All material from 2018-2019.
Fields: *CC_Number Exp CVV Name Country State City Address Zip Email_Phone*

An action of unprecedented generosity from AllWorld.Cards

Checking the validity of 98 random cards

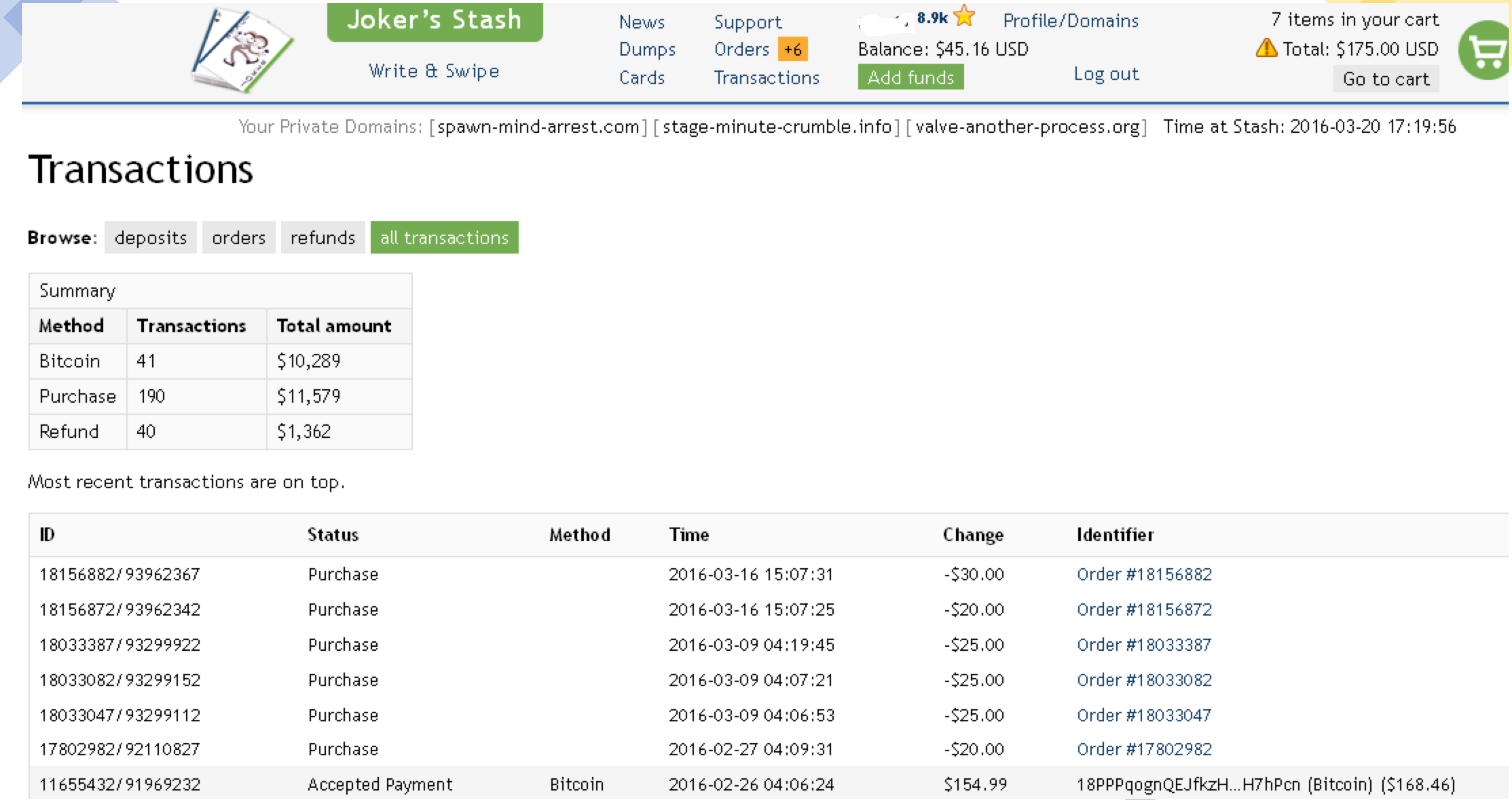
Checked: 98 of 98
Valid: 26 (27%)
Total cost: 12.90$

The password for the archive is the Tor domain.



Show 10 entries

PART NAME	BIN	DOE	CVV	HOLDER	BANK	CC BRAND	CC LEVEL	CC TYPE	COUNTRY	STATE	CITY	ZIP
10.0...	451140	06/23	+	+	BANC...	VISA	VISA	CRED...	Braz...	Cali...	Reed...	93654
10.0...	379136	12/24	+	+	YORK...	AMER...	AMER...	CRED...	Unit...	Cali...	Sali...	93908
10.0...	379003	12/22	+	+	TRAV...	AMER...	AMER...	DEBIT	Unit...	Arka...	Bent...	72712
10.0...	376792	07/22	+	+	GRCC	AMER...	AMER...	CRED...	Mexi...	Texas	Hous...	77057



[redacted] 8.9k

Balance: $45.16 USD

7 items in your cart

Total: $175.00 USD

Your Private Domains: [spawn-mind-arrest.com] [stage-minute-crumble.info] [valve-another-process.org] Time at Stash: 2016-03-20 17:19:56

Transactions

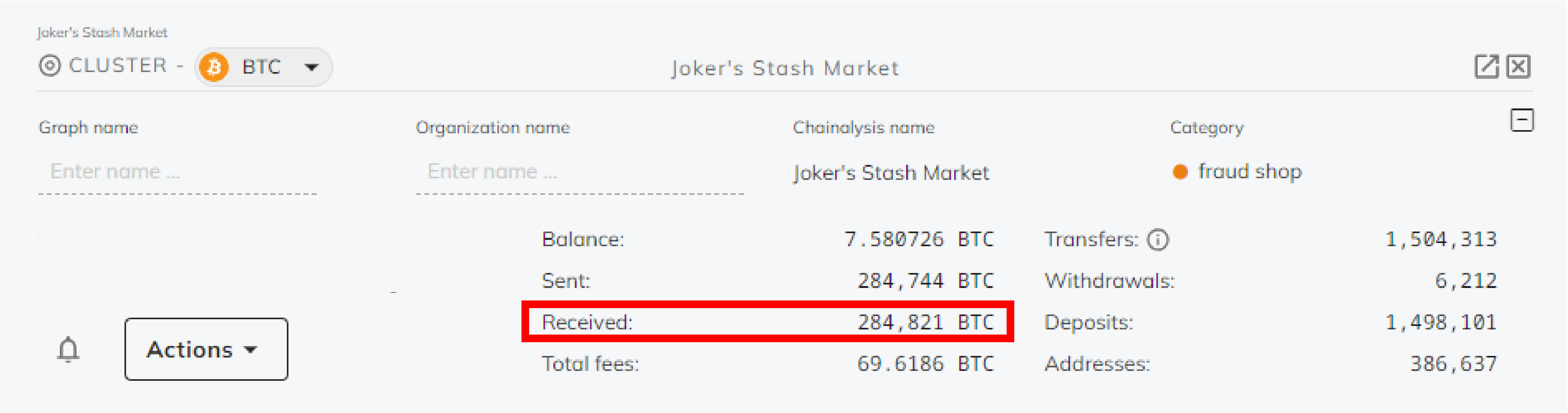
Browse: deposits orders refunds all transactions

Summary

Method	Transactions	Total amount
Bitcoin	41	$10,289
Purchase	190	$11,579
Refund	40	$1,362

Most recent transactions are on top.

ID	Status	Method	Time	Change	Identifier
18156882/93962367	Purchase		2016-03-16 15:07:31	-$30.00	Order #18156882
18156872/93962342	Purchase		2016-03-16 15:07:25	-$20.00	Order #18156872
18033387/93299922	Purchase		2016-03-09 04:19:45	-$25.00	Order #18033387
18033082/93299152	Purchase		2016-03-09 04:07:21	-$25.00	Order #18033082
18033047/93299112	Purchase		2016-03-09 04:06:53	-$25.00	Order #18033047
17802982/92110827	Purchase		2016-02-27 04:09:31	-$20.00	Order #17802982
11655432/91969232	Accepted Payment	Bitcoin	2016-02-26 04:06:24	$154.99	18PPPqognQEJfkzH...H7hPcn (Bitcoin) ($168.46)



Joker's Stash Market

CLUSTER - BTC

Joker's Stash Market

Graph name	Organization name	Chainalysis name	Category
Enter name ...	Enter name ...	Joker's Stash Market	● fraud shop

Balance:	7.580726 BTC	Transfers:	1,504,313
Sent:	284,744 BTC	Withdrawals:	6,212
Received:	284,821 BTC	Deposits:	1,498,101
Total fees:	69.6186 BTC	Addresses:	386,637

🃏 Since 22 Augst 2013

- Joker’s Stash Wallet
  Received: 284,821 Bitcoin

Quick Maffs

- Which would currently be worth around:
  £6.45 Billion 🤑 💸 💰

Payment Card Breaches

The cyberattacks resulted in the theft of some 160 million credit card numbers

The attackers mostly exploited SQL injection vulnerabilities in the targeted companies' computers

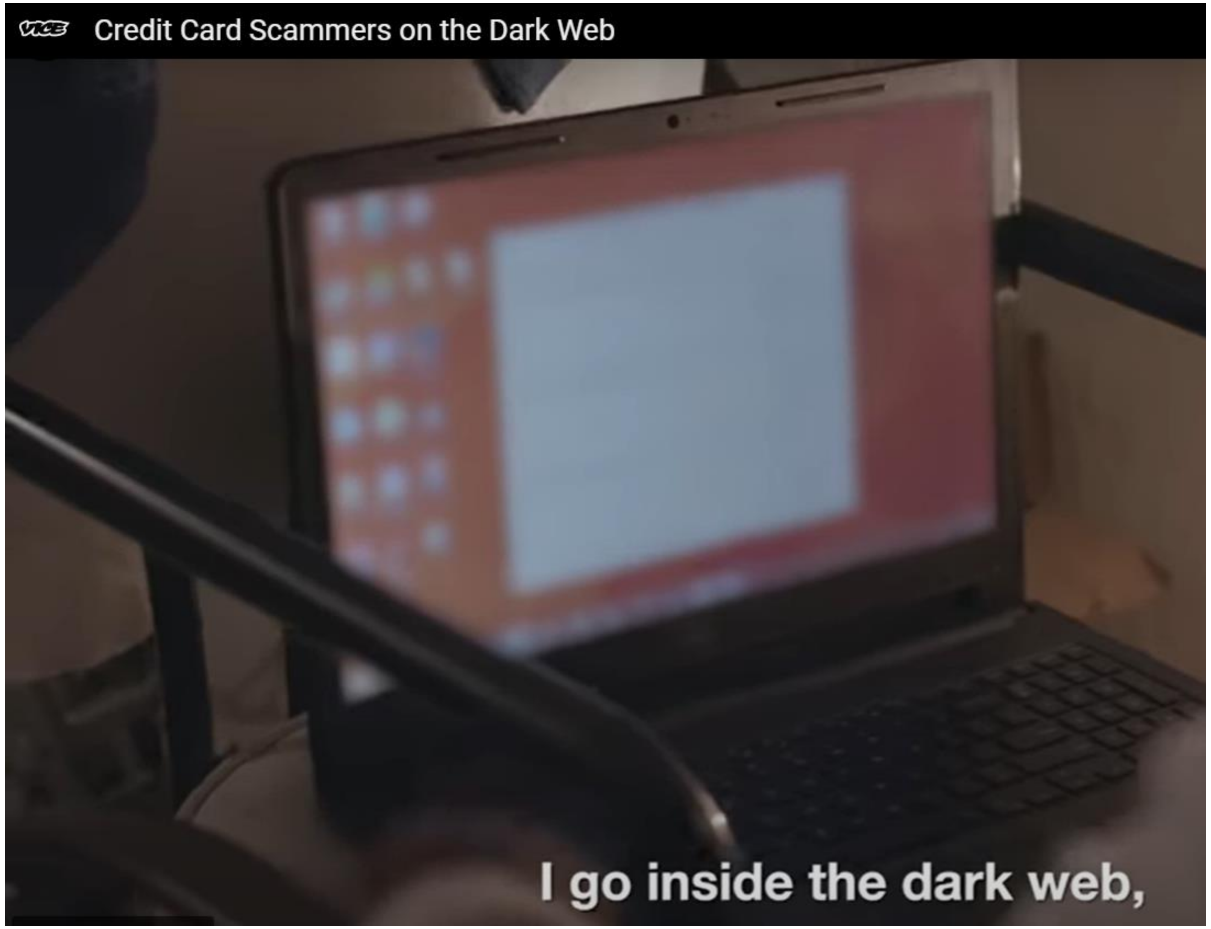
They then planted backdoor malware that provided them a foothold in the network, in some cases for more than a year.

They employed "sniffer" programs to root out and pilfer the data, storing the stolen information in systems scattered around the globe.

A team of cybercriminals stole data from:

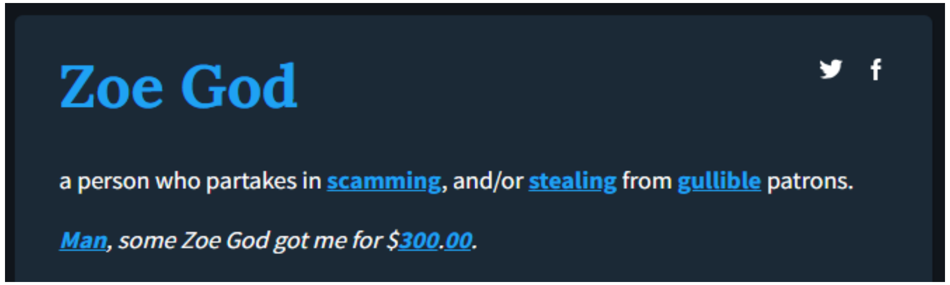
- Heartland
- NASDAQ
- 7-Eleven
- Carrefour
- JCP
- Hannaford
- Dow Jones
- Wet Seal
- Commidea
- Dexia
- JetBlue
- Euronet
- Visa Jordan
- Global Payment
- Diners Singapore
- Ingenicard.

Buying & Using the “Fullz”



Credit Card Scammers on the Dark Web

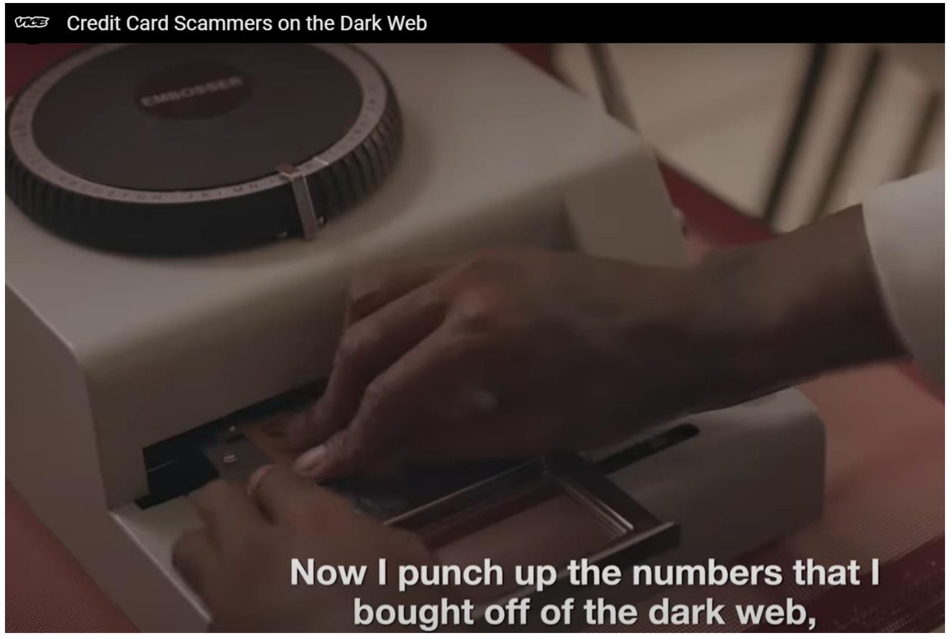
I go inside the dark web,



Zoe God

a person who partakes in scamming, and/or stealing from gullible patrons.

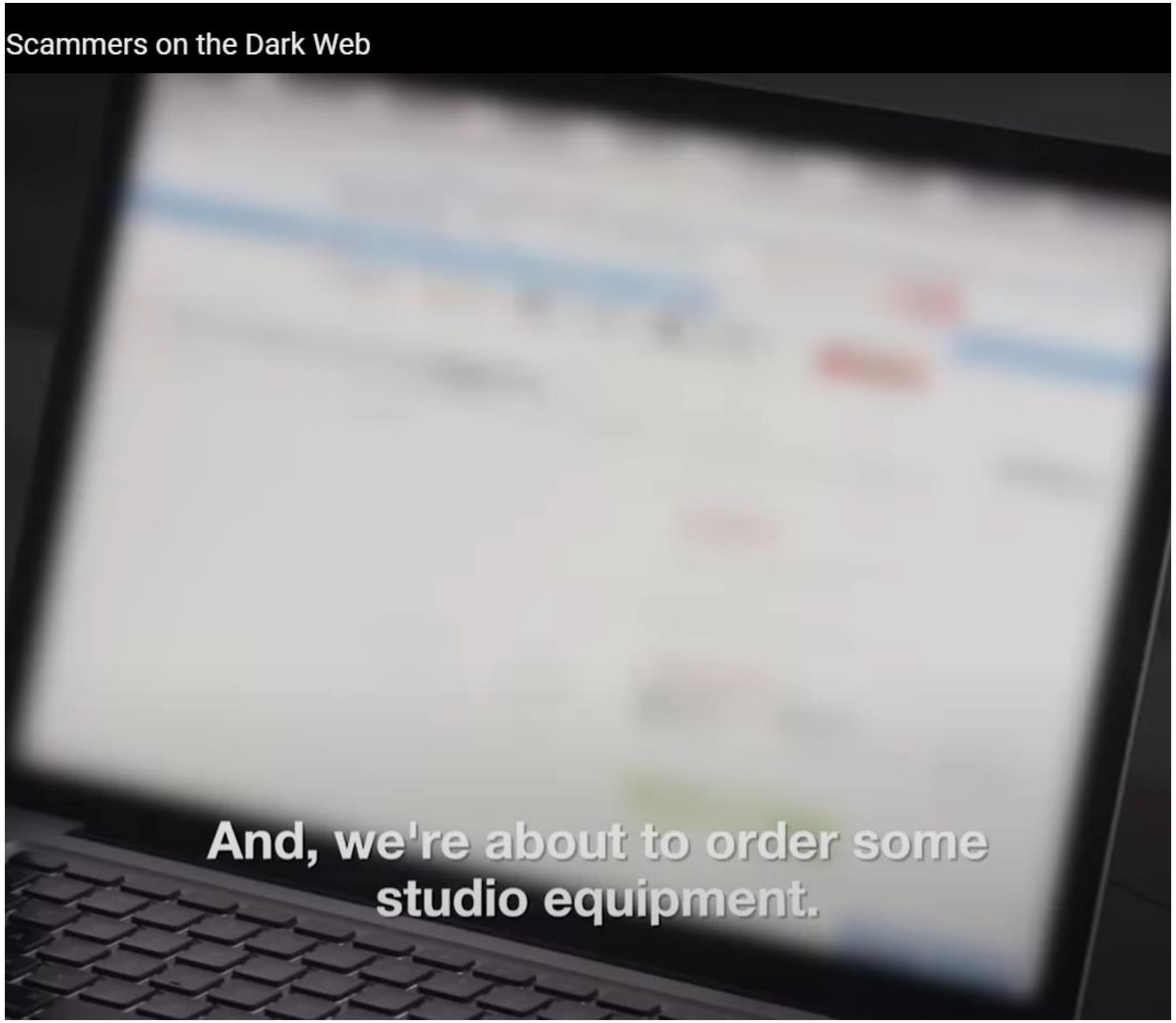
Man, some Zoe God got me for $300.00.



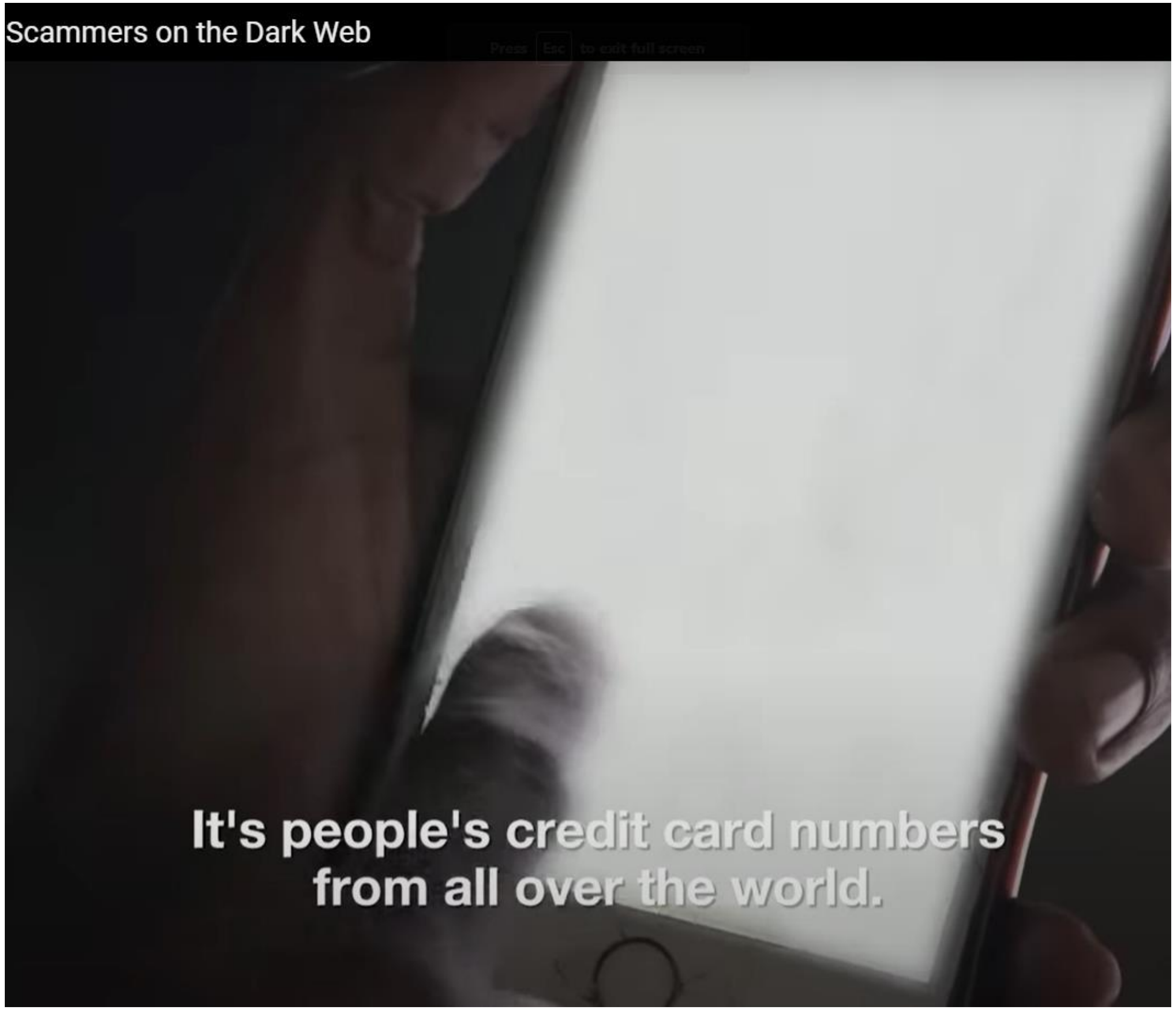
Credit Card Scammers on the Dark Web

Now I punch up the numbers that I bought off of the dark web,

Card-Not-Present (CNP) purchases



And, we're about to order some studio equipment.



It's people's credit card numbers from all over the world.