/ How API flaws led to admin access to over 1,000 USA dealers and control over your car /



Eaton Zveare | DEF CON 33 (CHV) | August 8, 2025

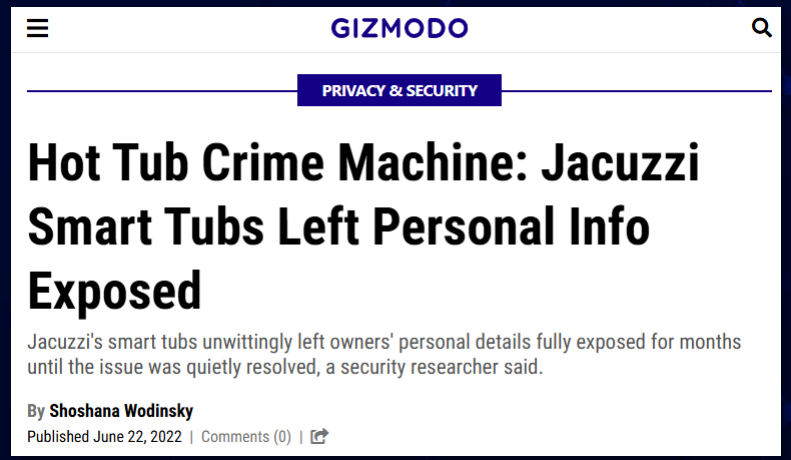
EATONWORKS

harness

/ me

- A constant thorn in automakers' side (:
- Started with game hacking (Game Shark, Action Replay, Xbox modchips)
- First big automaker hack (Toyota supplier network) blew up in the news

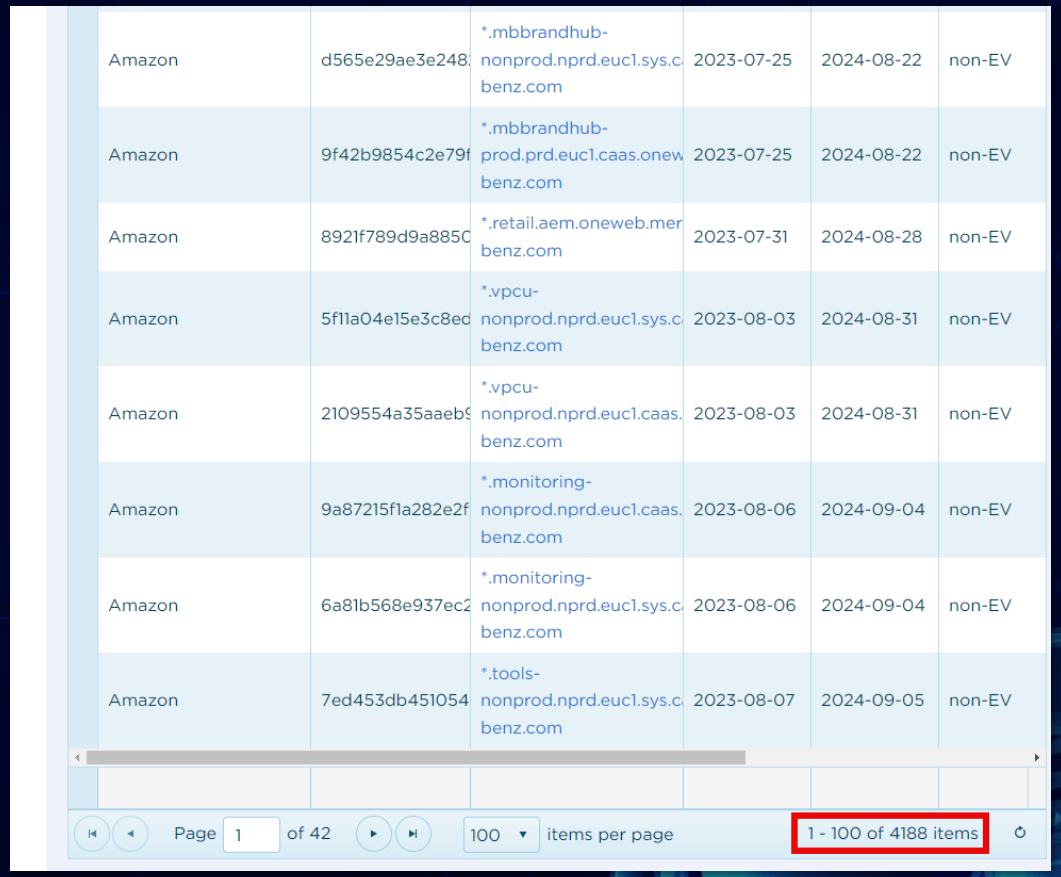




McDelivery

/ Automaker Motivation

- Just for fun!
- Started with Toyota (we own Toyota cars)
- Lots of domains = big attack surface



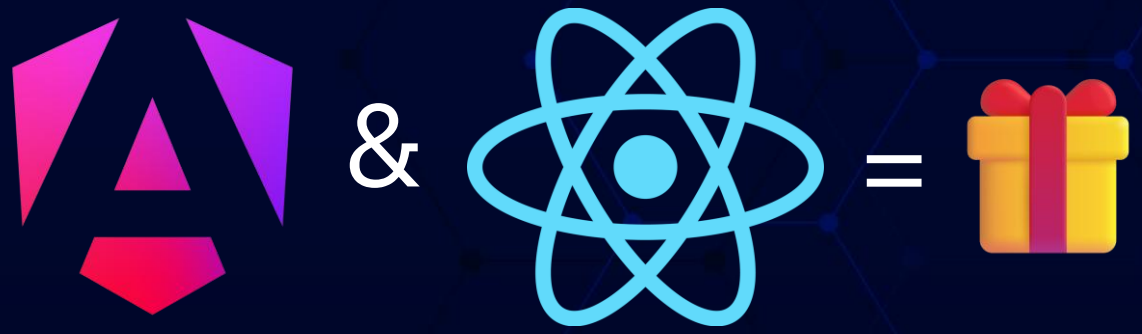
Amazon	d565e29ae3e248	*.mbbrandhub-nonprod.nprd.euc1.sys.c benz.com	2023-07-25	2024-08-22	non-EV
Amazon	9f42b9854c2e79f	*.mbbrandhub-prod.prd.euc1.caas.onew benz.com	2023-07-25	2024-08-22	non-EV
Amazon	8921f789d9a885(	*.retail.aem.oneweb.mer benz.com	2023-07-31	2024-08-28	non-EV
Amazon	5f11a04e15e3c8ed	*.vpcu-nonprod.nprd.euc1.sys.c benz.com	2023-08-03	2024-08-31	non-EV
Amazon	2109554a35aaeb9	*.vpcu-nonprod.nprd.euc1.caas. benz.com	2023-08-03	2024-08-31	non-EV
Amazon	9a87215f1a282e2f	*.monitoring-nonprod.nprd.euc1.caas. benz.com	2023-08-06	2024-09-04	non-EV
Amazon	6a81b568e937ec2	*.monitoring-nonprod.nprd.euc1.sys.c benz.com	2023-08-06	2024-09-04	non-EV
Amazon	7ed453db451054	*.tools-nonprod.nprd.euc1.sys.c benz.com	2023-08-07	2024-09-05	non-EV

Page 1 of 42 100 items per page 1 - 100 of 4188 items

CT logs from an automaker showing thousands of subdomains.

/ What I look for

- JS heavy apps (especially with source maps)
- Ripe for API and secret discovery
- Admin functionality can also be uncovered
  - Remember this point!



Angular & React apps are great hack targets!

/ What I hacked

- ✨ **Brand new, DEF CON 33-exclusive vulnerability disclosure!** ✨
- Found vulnerabilities in top automaker’s centralized dealer platform
- Used by automaker’s authorized dealers in the USA
- End result: creation of national admin account
- Full access to ***over 1,000*** USA dealers
- Could start your car, get your personal info, & more



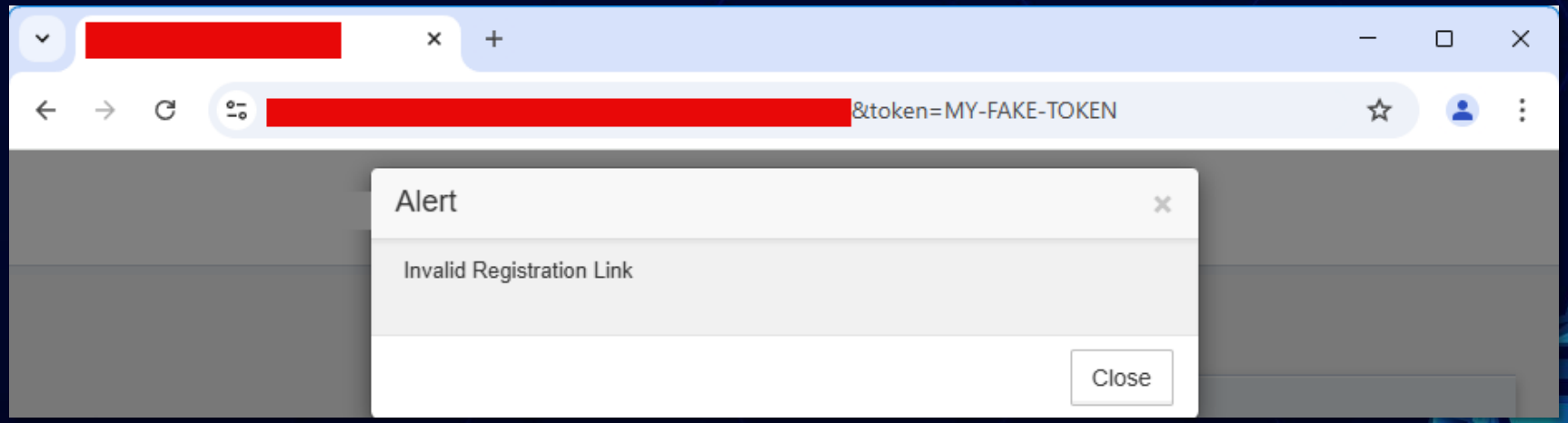
/ Dealer System Details

- Used to order cars, make sales, manage customers/leads, etc
- Accessible via internet
- Cornerstone of day-to-day operations
- Invite only, no open registration
- Uses two-factor auth
- SAP/Java with AngularJS frontend



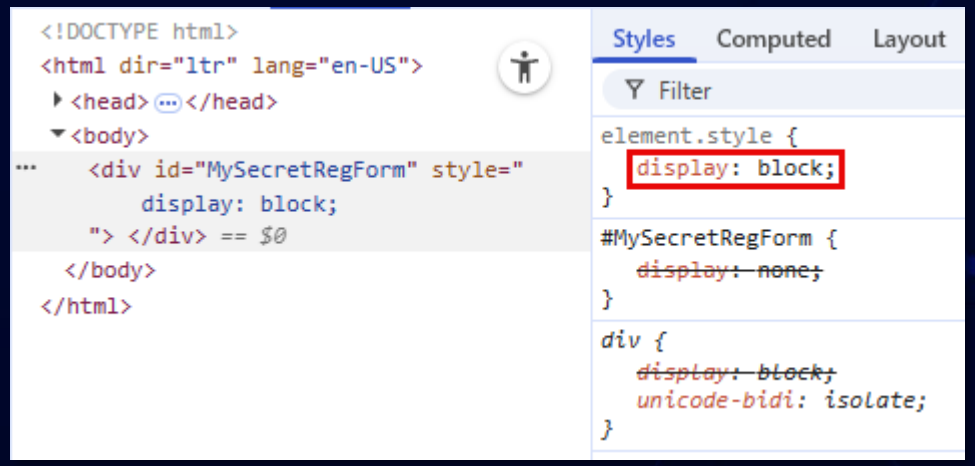
/ The Invite System

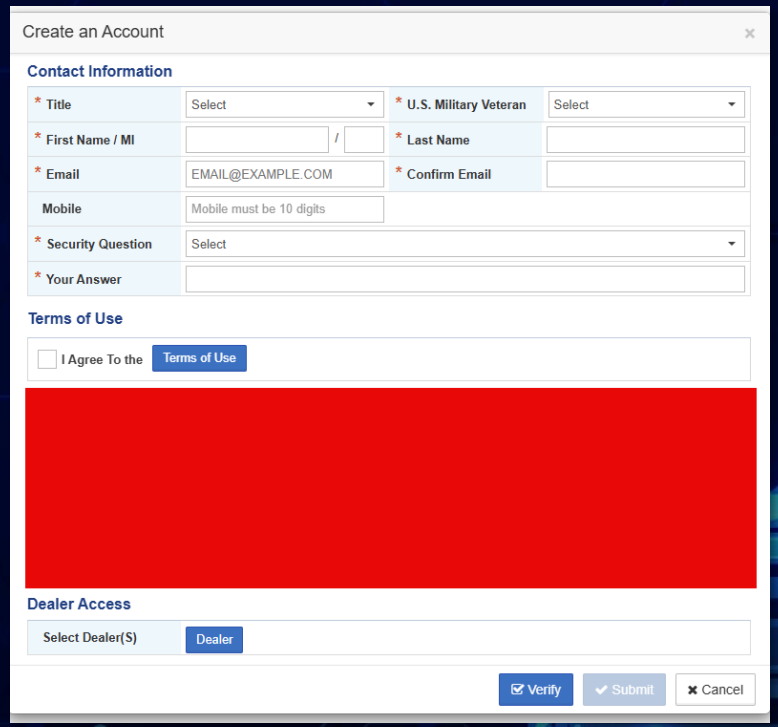
- New employee? Dealer admin invites you via email
- Email has unique invite token in link
- Login page has JS to call server-side token validation API
  - Valid token? Registration form shown
  - Bad token? Error!



/ CSS’ing the registration form

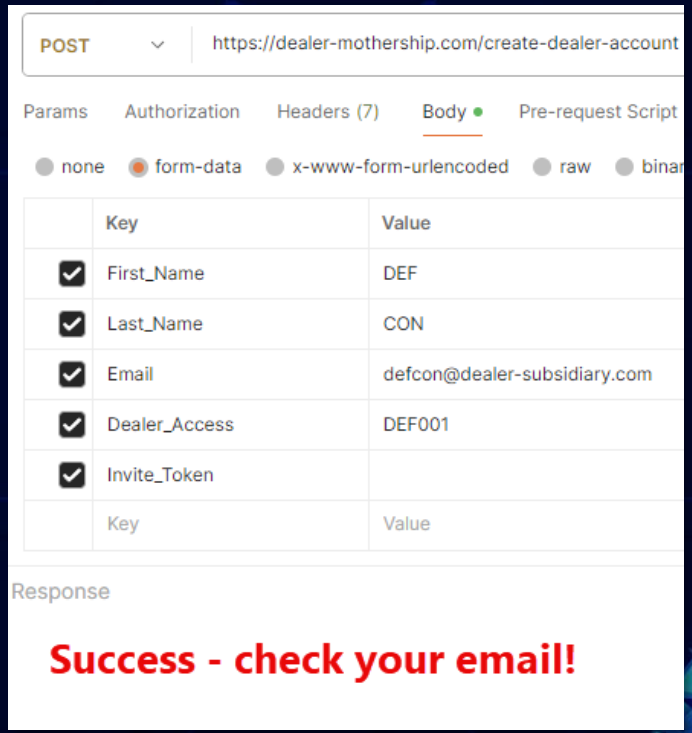
- Can’t forge token = can’t pass API check
- Discovery: hidden registration form in HTML
- Hack: apply “*display: block;*” using Chrome devtools
  - Same end result as passing API check





/ Submitting the registration

- Bad news: Form POST fields include invite token
- Good news: Server doesn’t check it!
- Can be blank - anyone could register!



Pseudo example in Postman

/ Congratulations! (maybe?)

BACK TO LIST Delete Source

noreply@[redacted]

Date: 26-01-2025 22:11:56

Subject: Your Account!



Congratulations!

You are receiving this email because your profile has been updated. You have completed the registration for a new [redacted]. This ID will allow you to access [redacted] and other related systems.

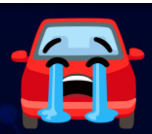
Please, **DO NOT SHARE** this ID with other people. Use the below URL to access the application and change your temporary password.

Please Note: You will not be able to log in to [redacted] until your Dealer Admin grants you the proper access.

SYSTEM ACCESS INFORMATION



Authentication failed. Not assigned the requested dealership or Dealer Code incorrect. If this problem persists, contact your dealer administrator.





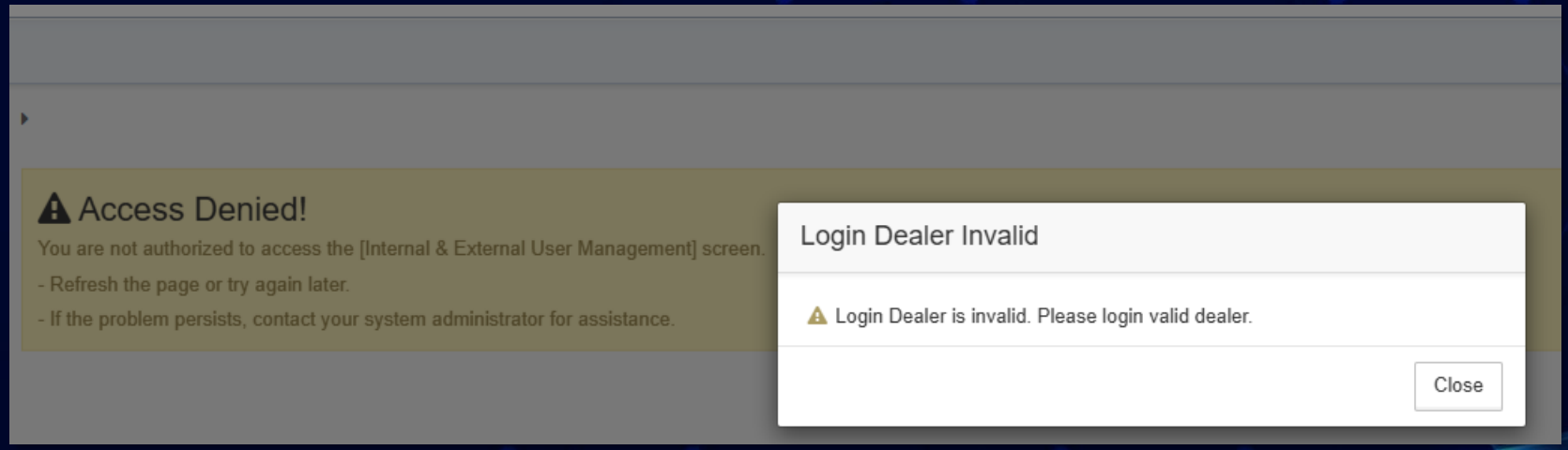
/ What now?

- Account useless - no permissions, no chance of approval
- Almost moved on/gave up
- Login page - limited attack surface
- Rest of site login-protected
- Valid session needed to poke further



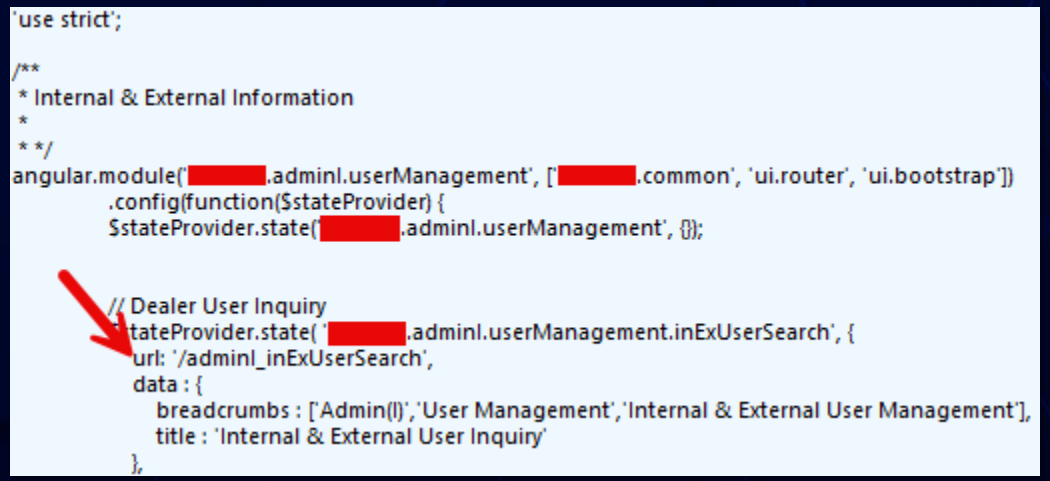
/ Profile update breakthrough

- Normal login would not establish a session
- “Profile update” option **did** establish a session! (JSESSIONID)
- Opened the door a tiny bit. Front end now loads!



/ New attack surface

- *Hundreds* of scripts containing APIs/pages ripe for exploit
- Previously unobtainable
- Valid session = hope of exploiting vulnerable APIs



```
'use strict';

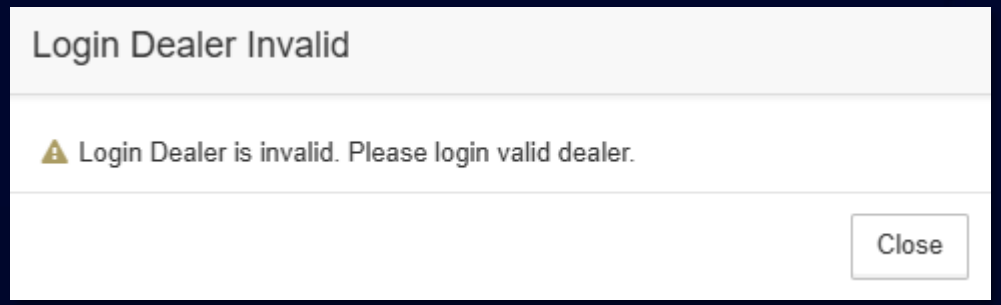
/**
 * Internal & External Information
 *
 * */
angular.module('[redacted].adminI.userManagement', ['[redacted].common', 'ui.router', 'ui.bootstrap'])
        .config(function($stateProvider) {
        $stateProvider.state('[redacted].adminI.userManagement', {});


        // Dealer User Inquiry
        $stateProvider.state( '[redacted].adminI.userManagement.inExUserSearch', {
            url: '/adminI_inExUserSearch',
            data : {
                breadcrumbs : ['Admin(I)','User Management','Internal & External User Management'],
                title : 'Internal & External User Inquiry'
            },
```

Discovered admin script

/ Accessing admin user management

- Can’t access normally; necessary to patch scripts to bypass errors
- First patch: comment out annoying popup
  - Patching done using Chrome Local Overrides.

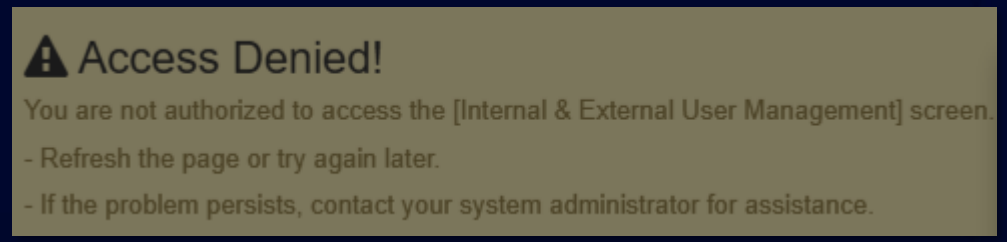



```
// Login Dealer Code Valid
/*if (retData.loginDealerCodeValid == false) {
    commonUtil.alertModalWarning({
        title: $rootScope.[redacted]Lang.common.tx_loginDealerInvalid,
        content: $rootScope.[redacted]Lang.common.tx_loginValidDealer,
        showClose: false
    });

    // Logout
    setTimeout(function(){
        commonUtil.clearToken();
        $('#logoff').submit();
    }, 5000);
}*/
```

/ Accessing admin user management

- Second patch: bypass access denied display
- Returning empty string means you have access




```
// Check State Valid
commonUtil.checkStateValid = function (stateName) {

    return '';

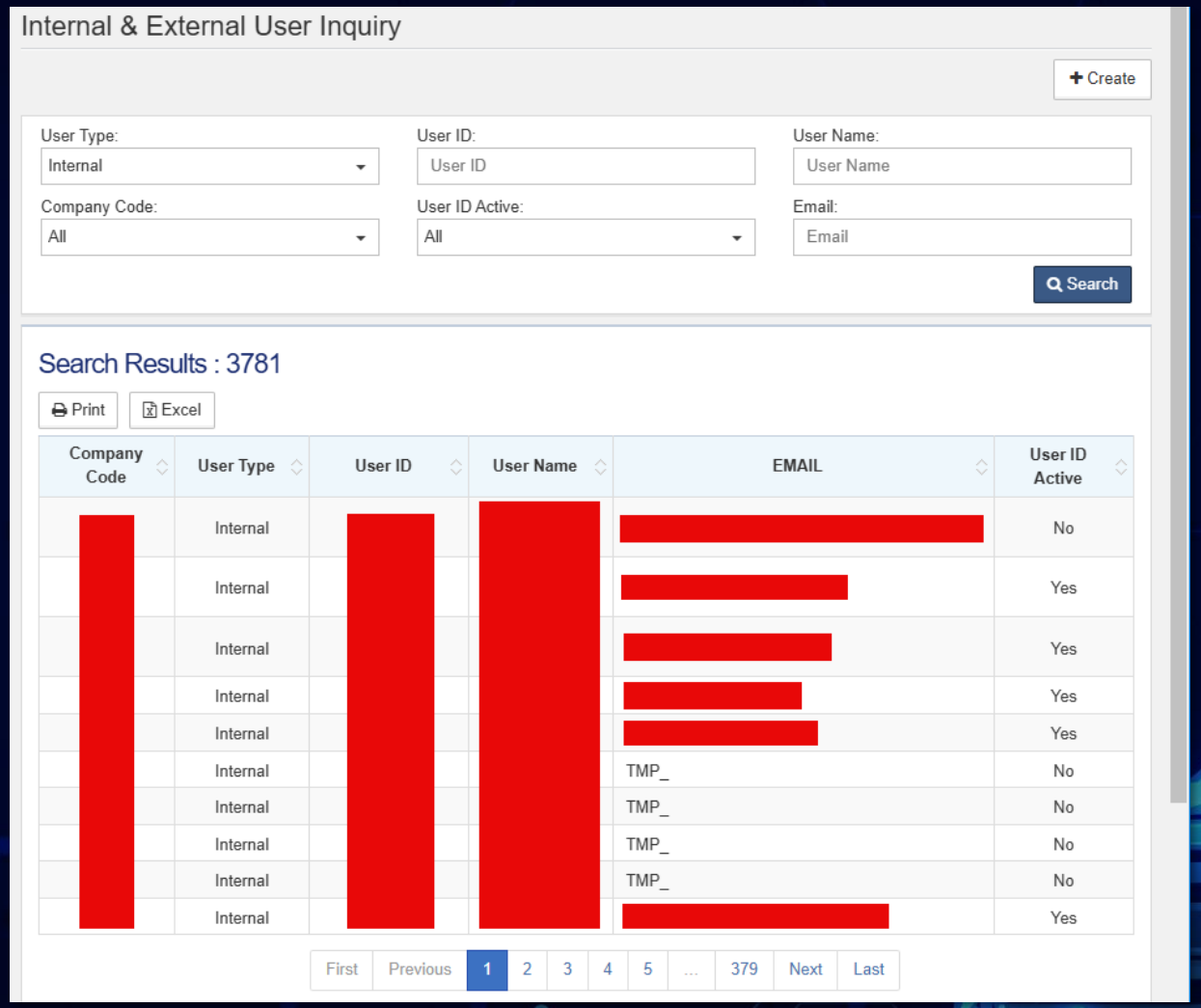
    if (stateName) {
        // New Popup
        if (stateName.indexOf('[redacted]Pop.') > -1 ) {
            return '';
        }

        // Sample
        if (stateName.indexOf('[redacted].sample.') > -1 ) {
            return '';
        }

        // Check only Sref Menu
        if (commonUtil.srefInfo && commonUtil.srefInfo[stateName]) {
            var dealerInfo = commonUtil.getDealerInfo();
            var userInfo = commonUtil.getUserInfo();
            var stateInfo = commonUtil.getMenuInfo(stateName);
            var stateTitle;
```

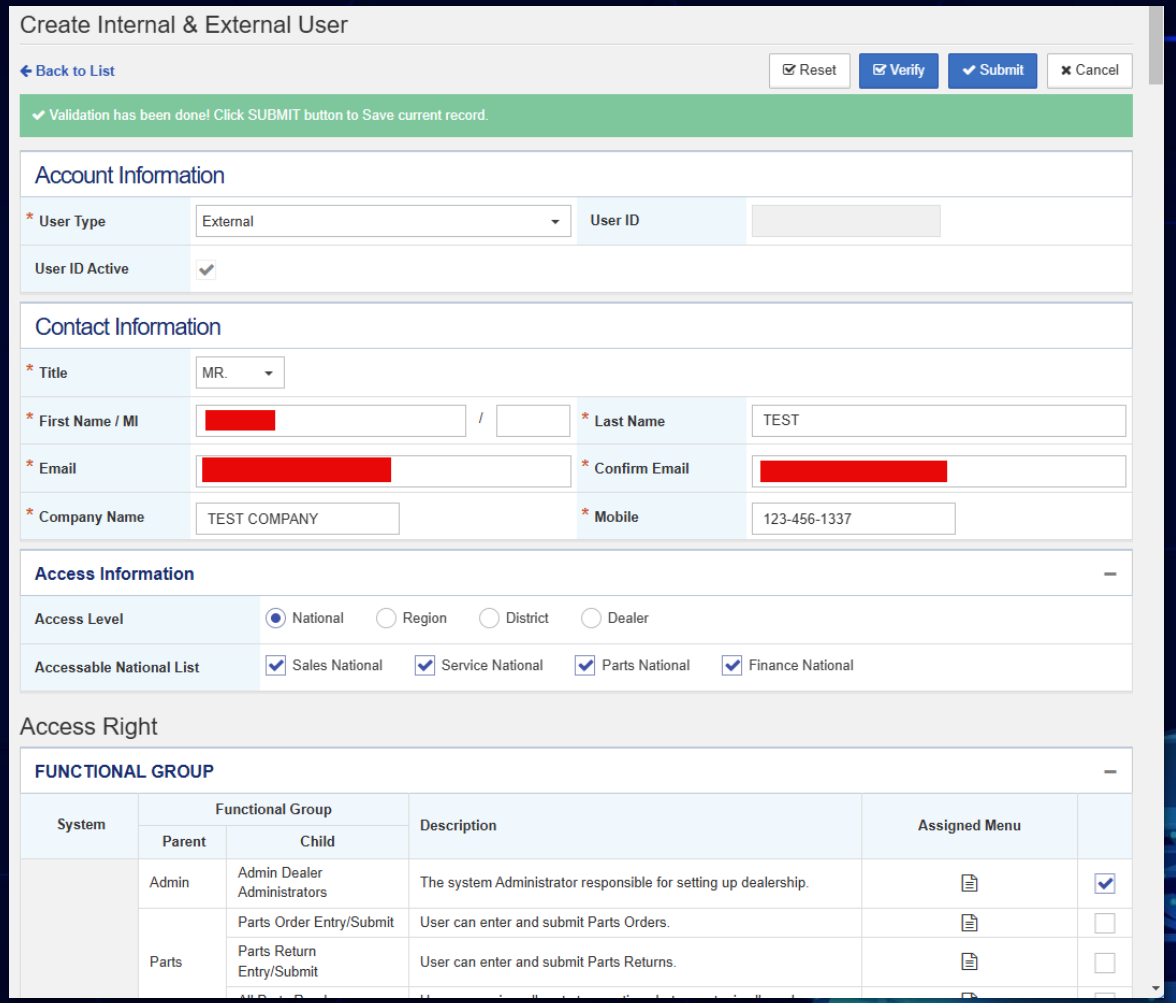
/ A welcome surprise

- 🚨 Users viewable!
- Note the create button...

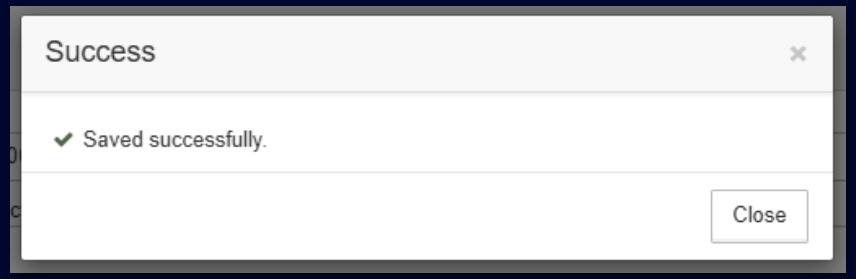


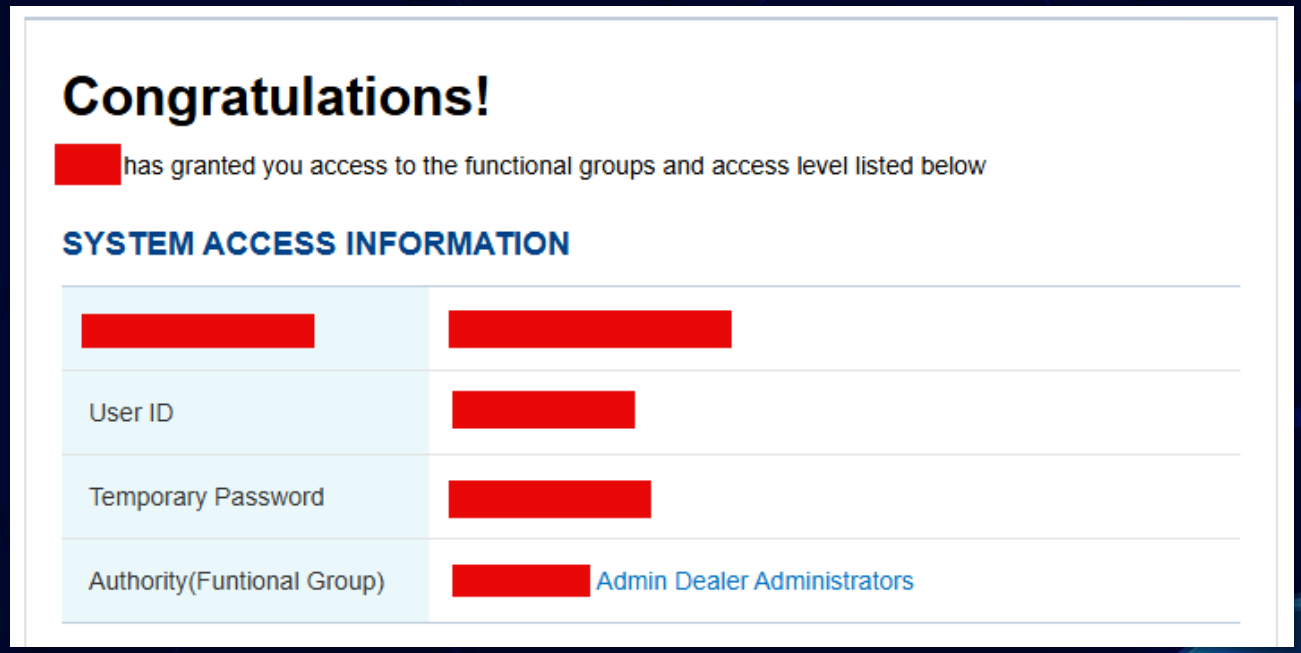
/ The create user form

- Juicy access options
- Access Rights = super long list
  - Like a CVS receipt
- Moment of truth: submit...



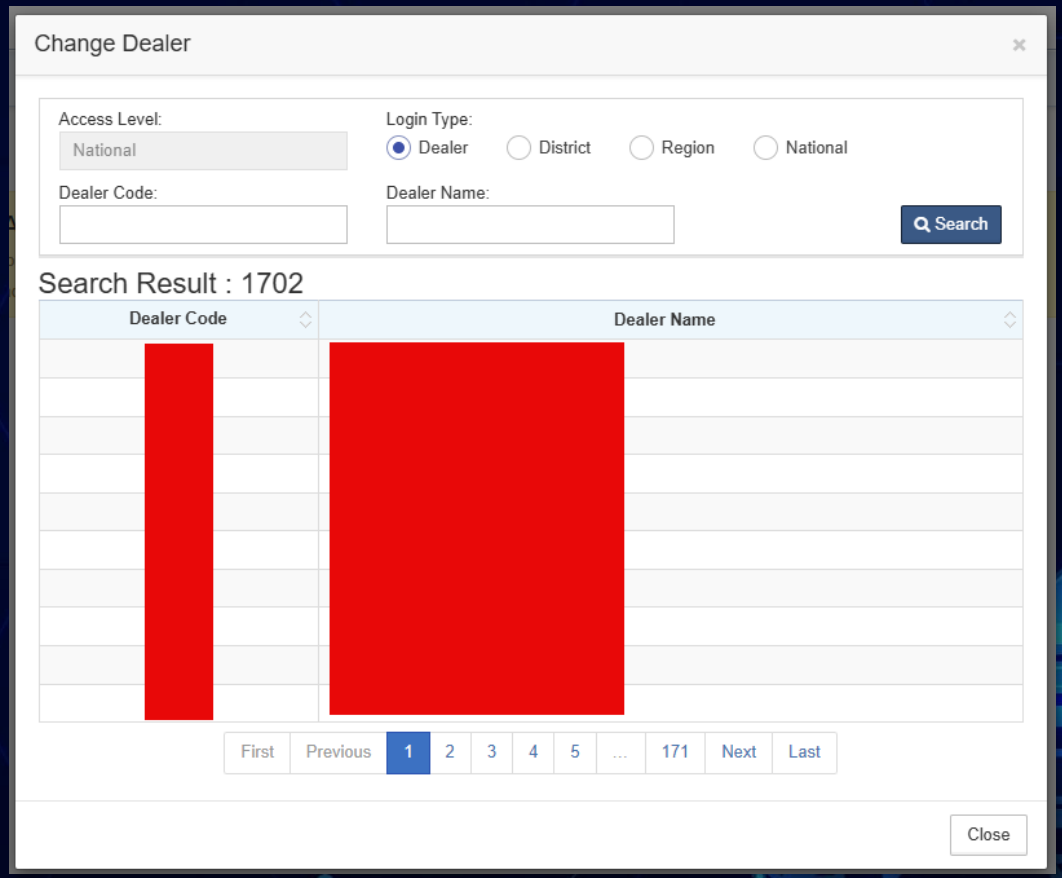
/ Congratulations! (for real)





/ The door is now open

- Account has access to **everything**
- First login: choose dealer to administer
- Let’s dig in…



/ Doxxing you from the parking lot

- Time for a real-world example!
- Weekend project: go to Publix and find a target. Took seconds to find.



Not a Cybertruck

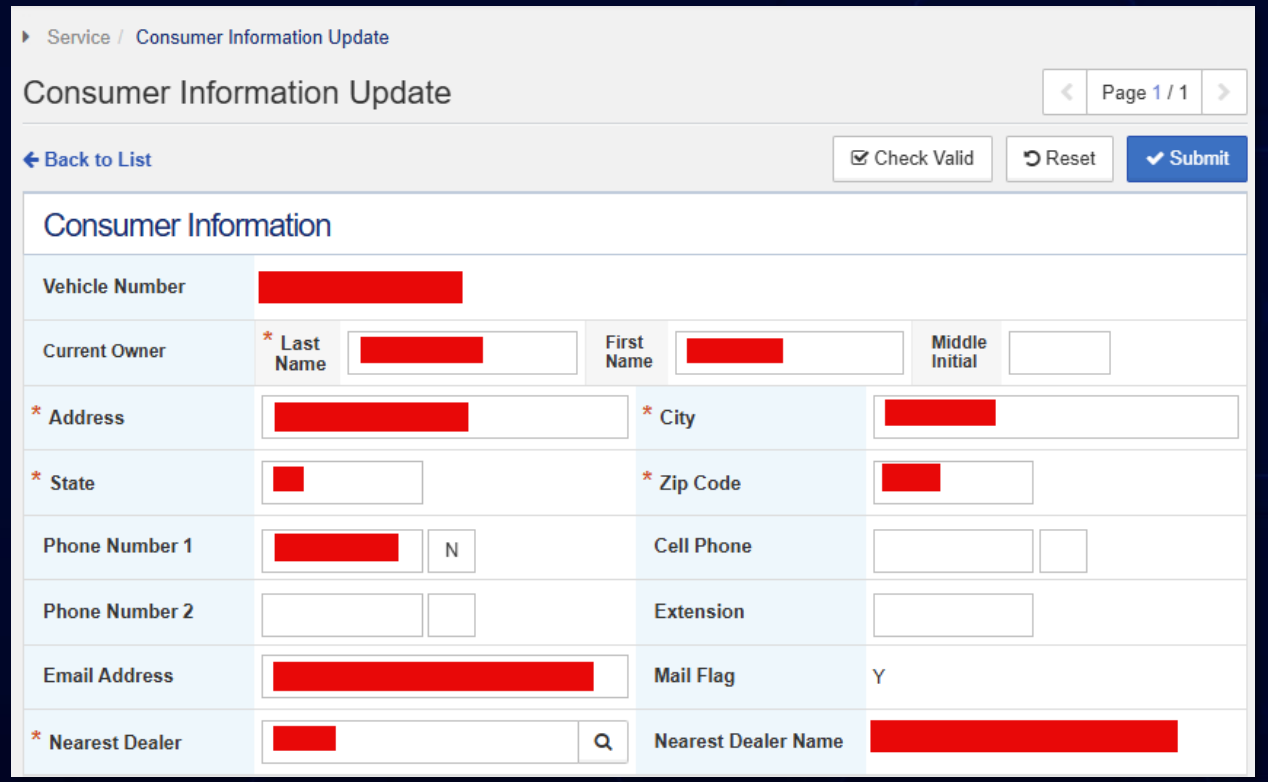
/ Doxxing you from the parking lot

- Swipe the VIN off the windshield real quick...
  - No amount of dirt can save you!



/ Doxxing you from the parking lot

- Consumer lookup/update tool exists in dealer system
- Supports lookup by VIN or first/last name
- Silent



/ Hacking a car

- Dealers have an enrollment systems to pair customers to their new car
- The pairing enables use of the mobile app
- Mobile app controls remote start and unlock functionality
- Pairing process could be abused to transfer ownership of cars



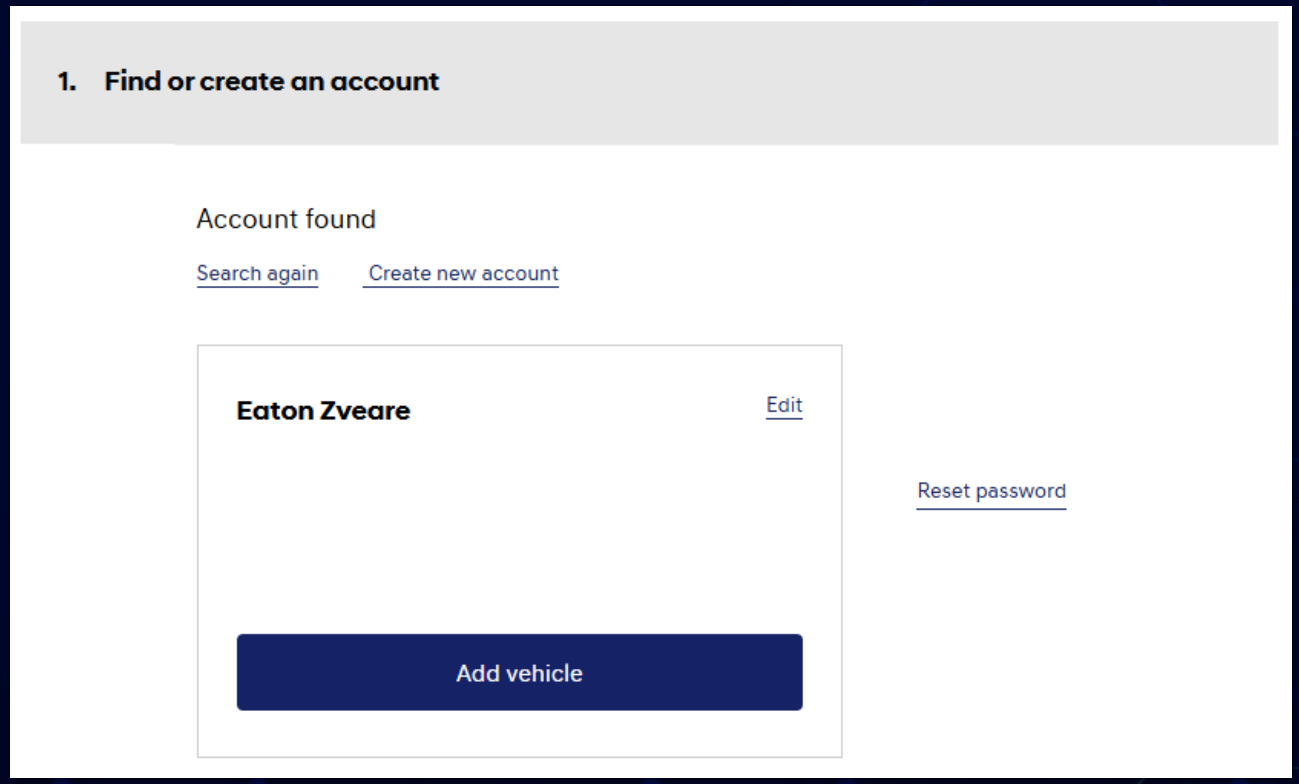
/ Hacking a car – prep

- Enlisted help of friend. Full consent obtained to test transfer
- I created fresh account on automaker’s consumer website
- Test goal: switch ownership of car to my fresh account



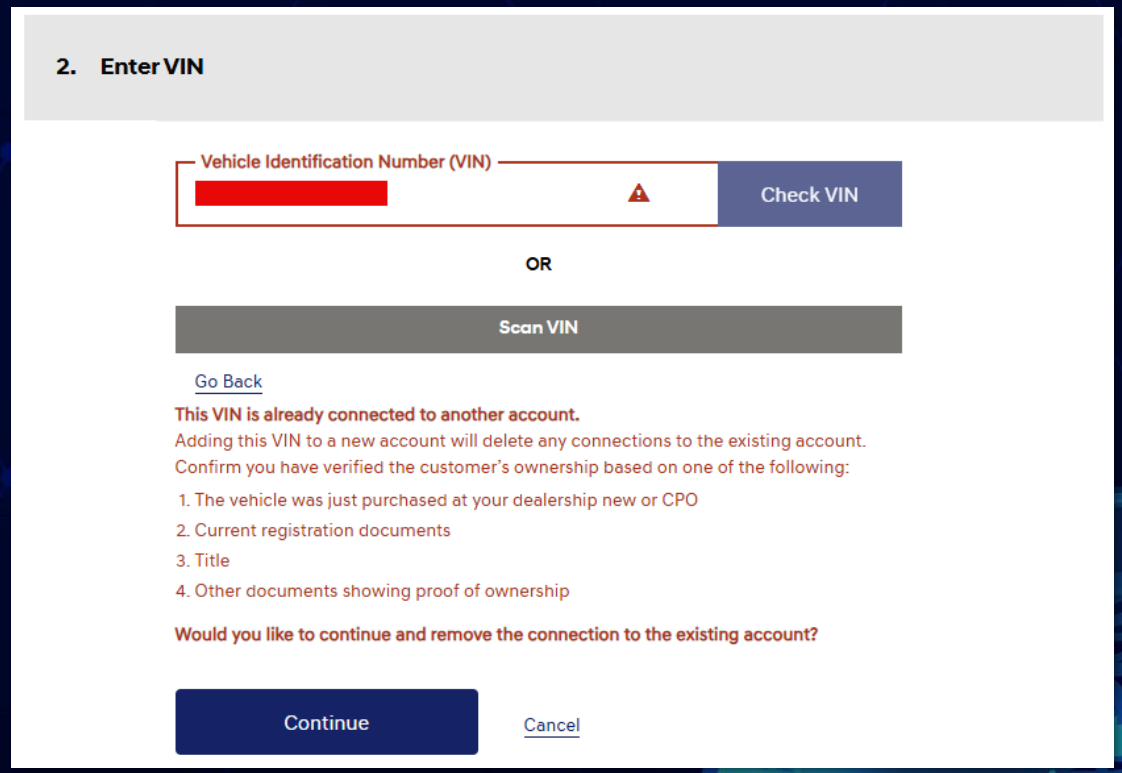
/ Hacking a car – step 1

- Log in to enrollment system using dealer account
- Find my consumer account to kick off the process



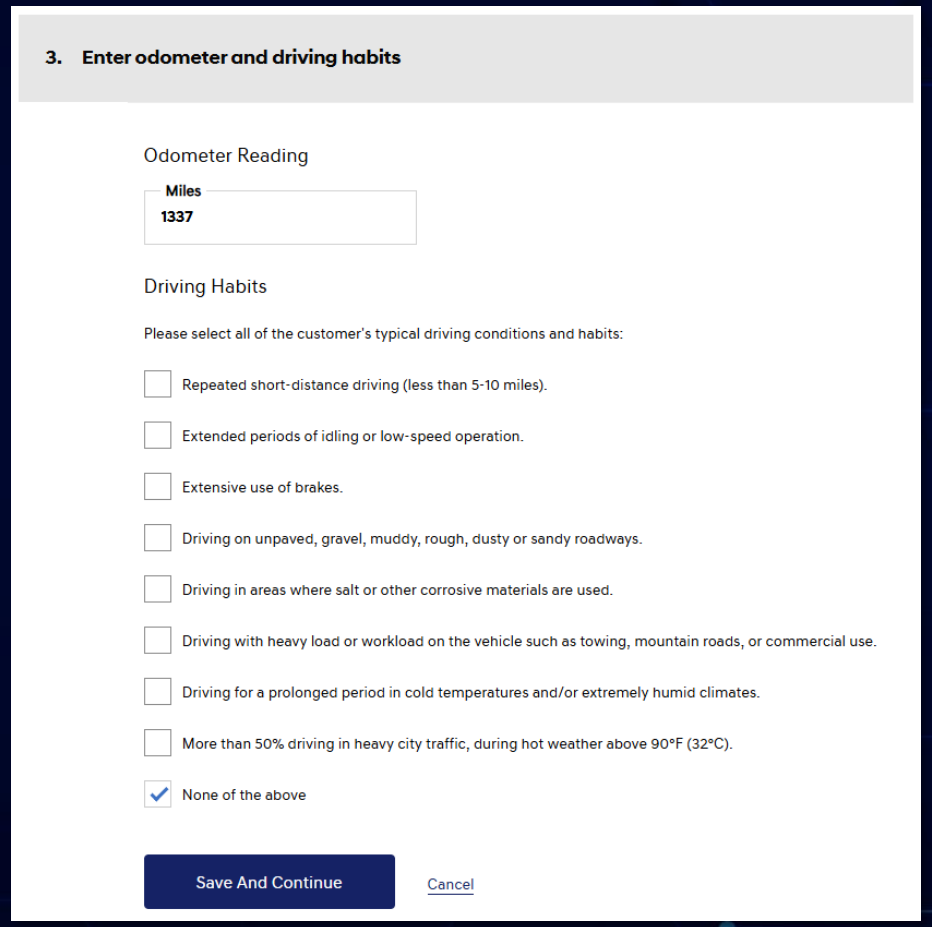
/ Hacking a car – step 2

- Obtain VIN. Can find on windshield
  - Remember: Consumer lookup tool supports lookup by name
- Enter VIN in form
- Pinky promise the request is legit 🤞



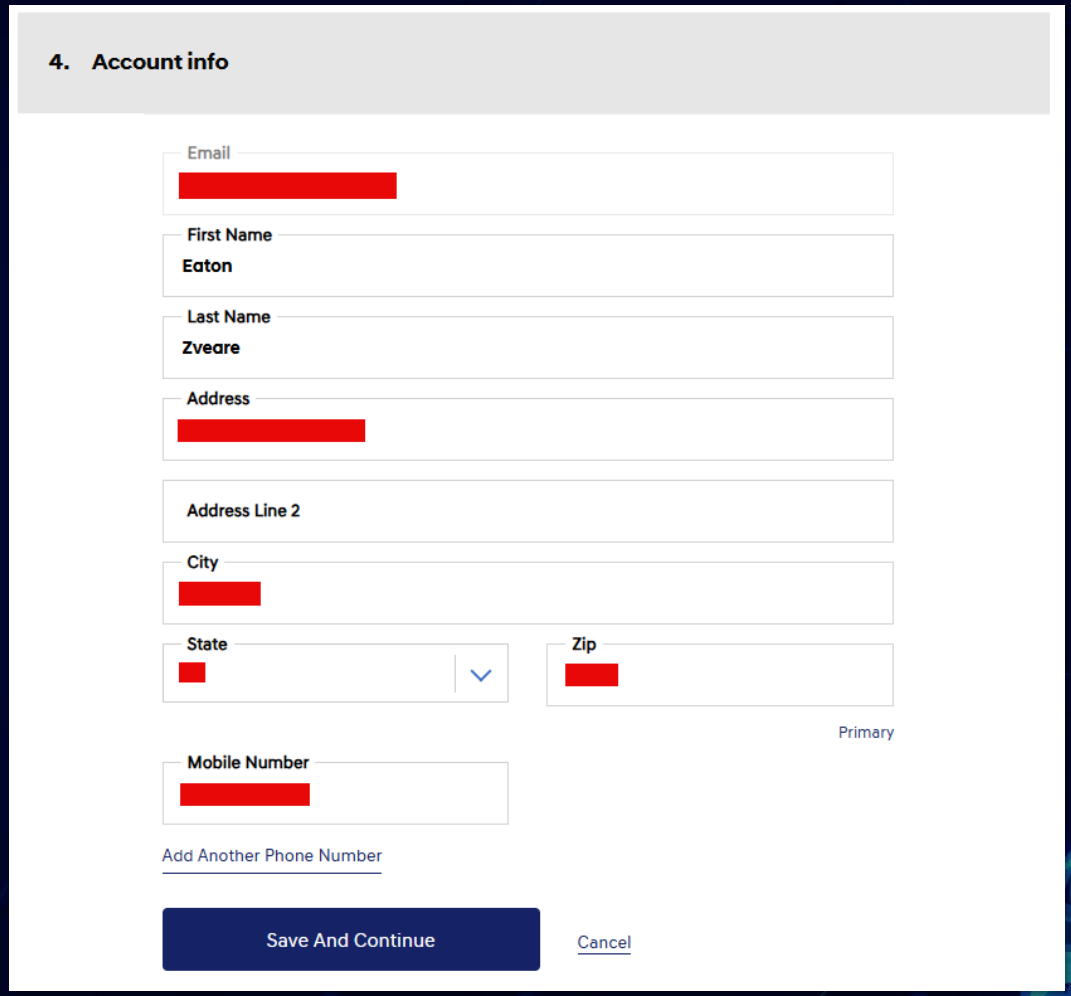
/ Hacking a car – step 3

- Grill the customer on their driving habits



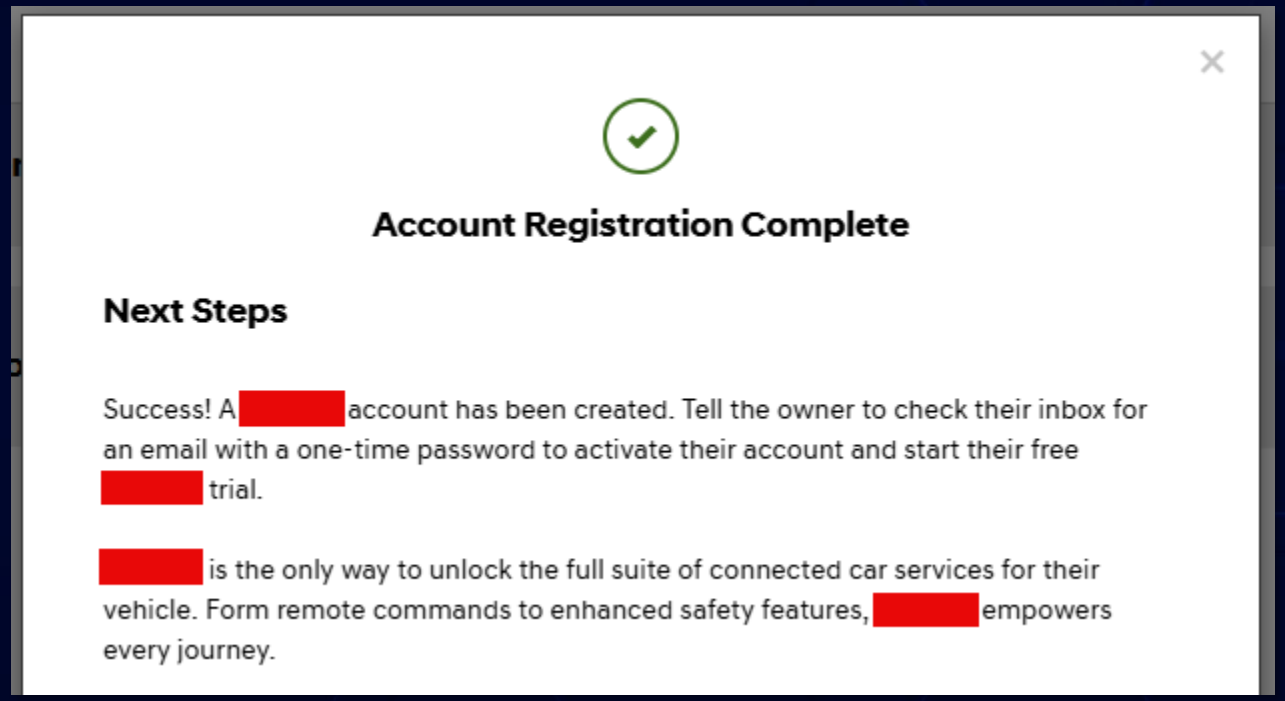
/ Hacking a car – step 4

- Confirm your account info



/ Hacking a car – success

- Ownership transfer complete



/ Hacking a car – control

- My account now owns the car
- To control it, mobile app is used
- Remote start, unlock, and location tracking confirmed working
- Car transferred back to friend without issue



/ Hacking a car – saying no

- Scenario: dealer offers to help set up your mobile app. You say no.
- Bad news: this makes things worse for you!
- Current owner gets email about transfer. You would **not** get it.
- Silent takeover of your car 

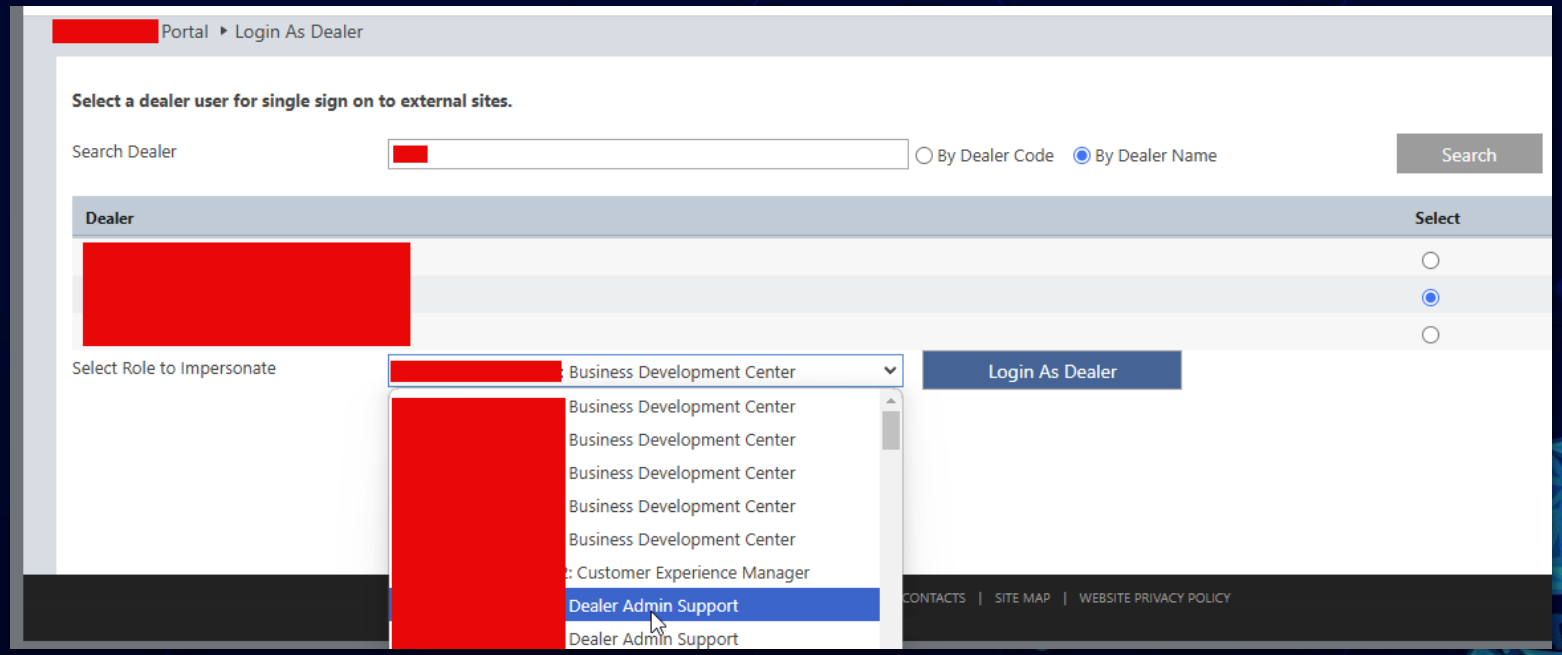
/ Hacking a car – takeaways

- Victim gets email alert, but powerless to stop transfer
- Enrollment system relies on dealer employee trust
- No owner would have thought of this as backdoor
- Affected cars: MY12 onwards
  - Standard telematics module = affects most cars you see
- Only needed to know the first/last name of your target



/ User impersonation

- Bombshell discovery: user impersonation feature
- Unlocked remaining systems
- Bypassed login & 2FA



/ Access Review

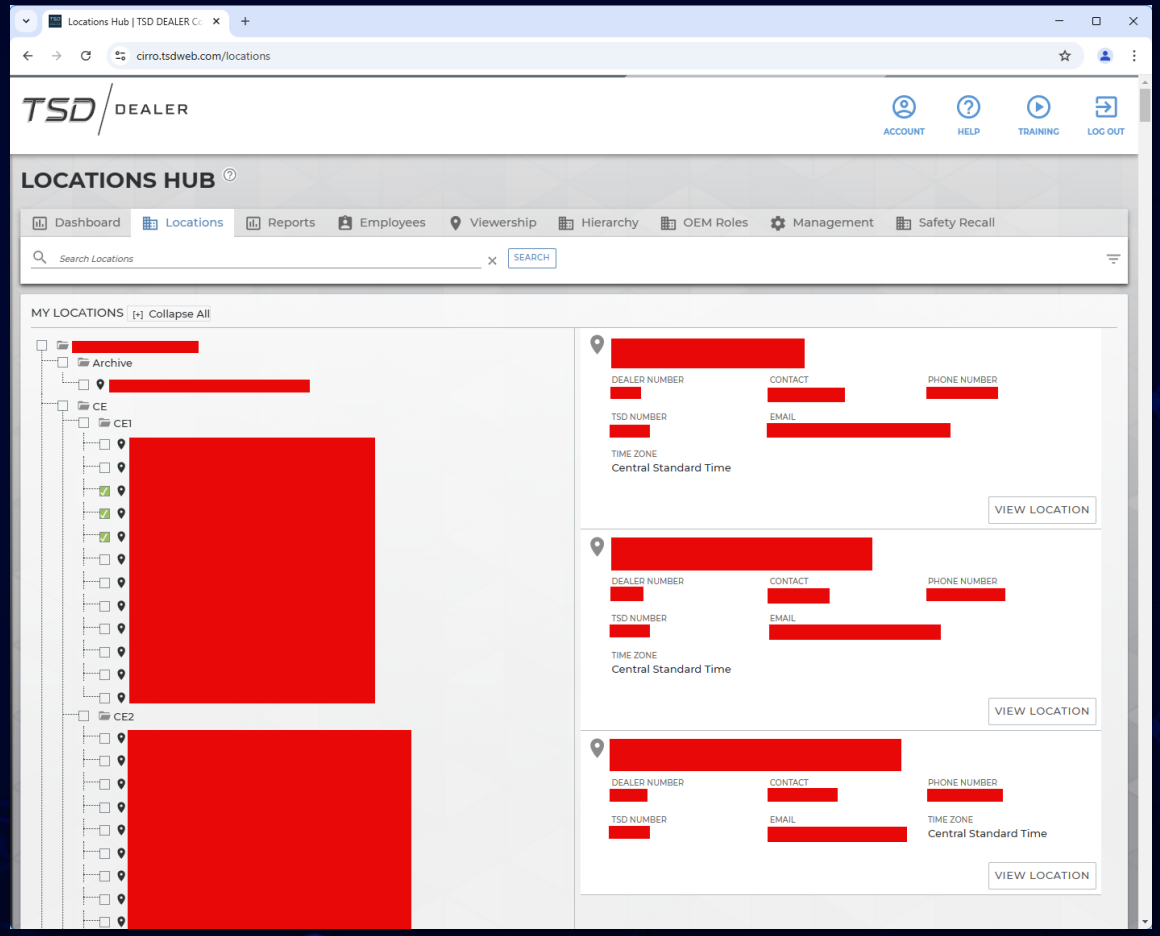
- National admin had access to *everything* (root-like)
- SSO into any system
  - Impersonate other users when necessary
- Let’s explore some highlights!



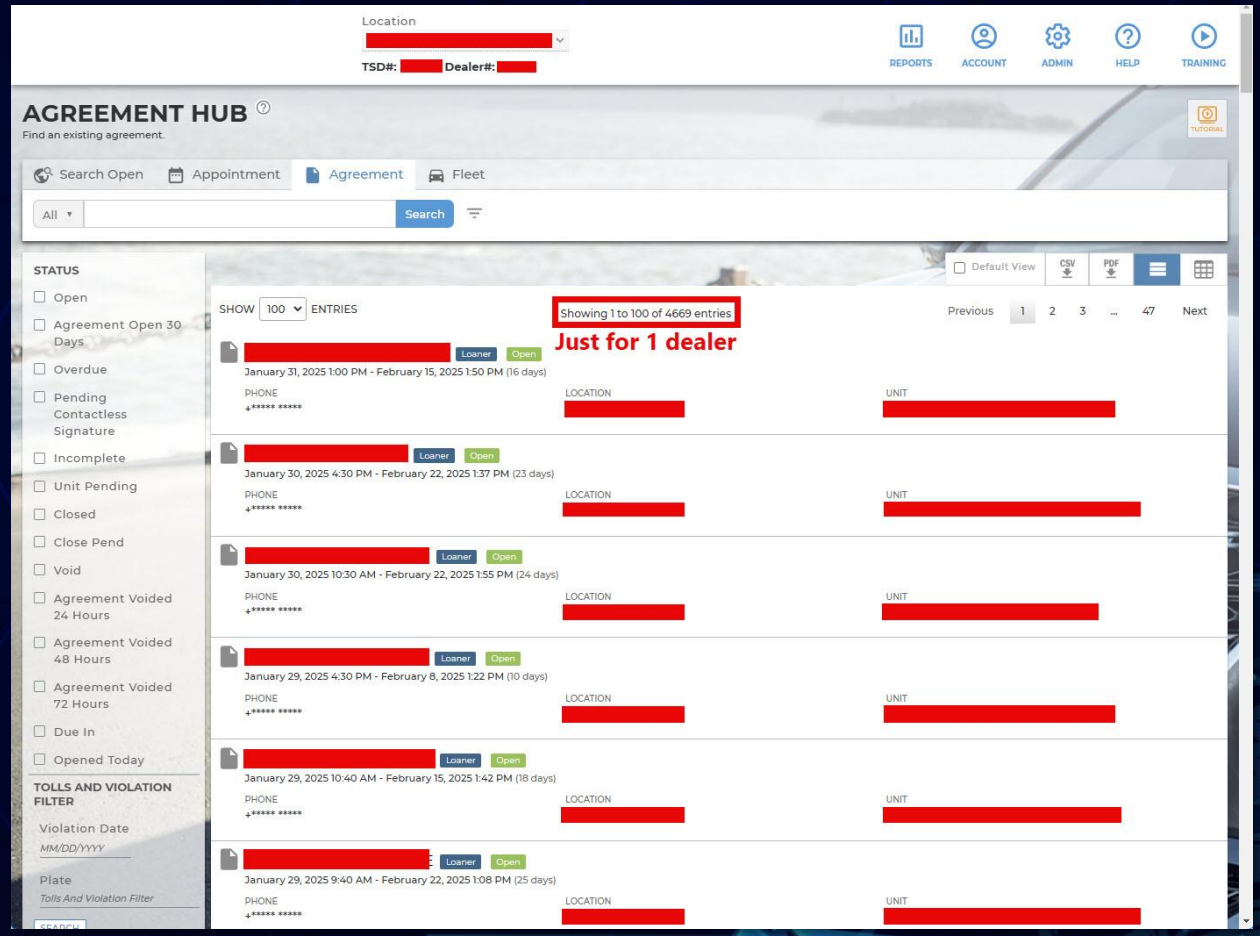
/ TSD Dealer Admin

- Loaner/courtesy vehicle platform.

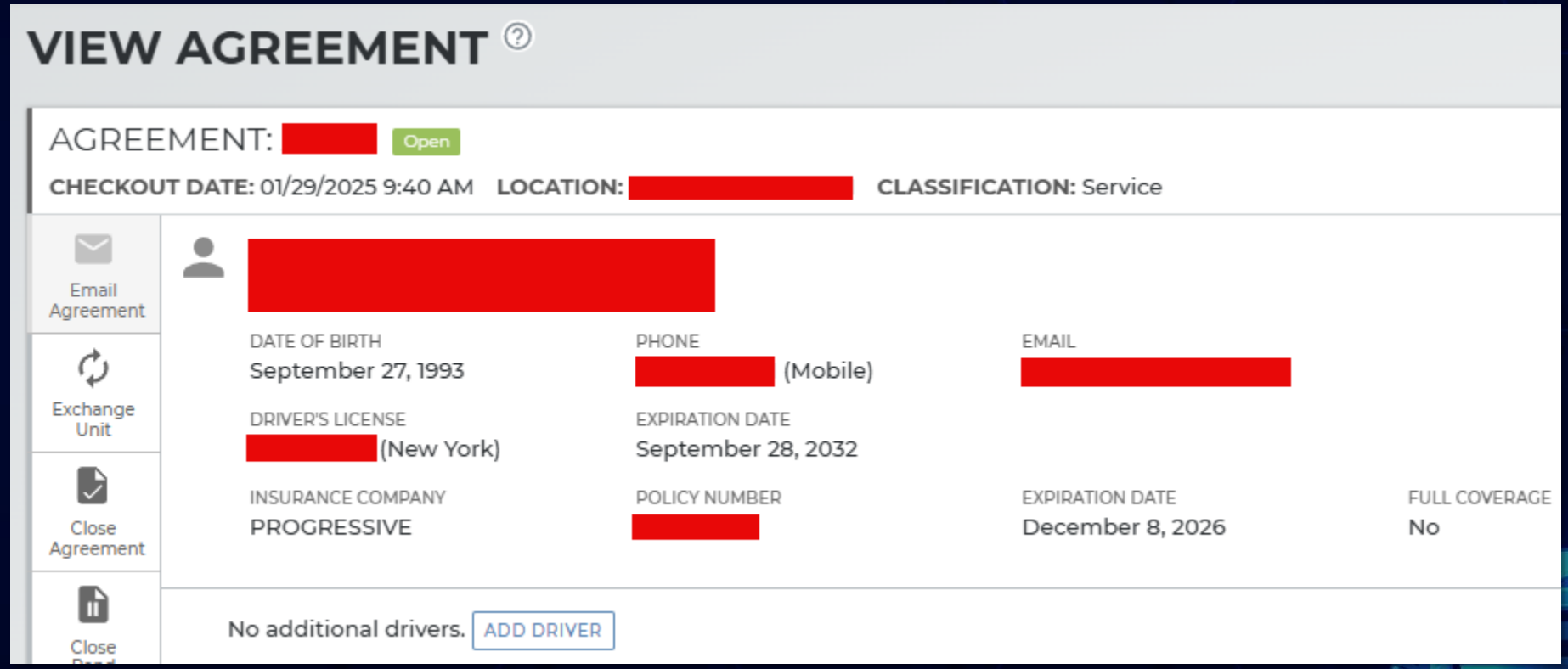
Choose any dealer



Viewing loaner agreements

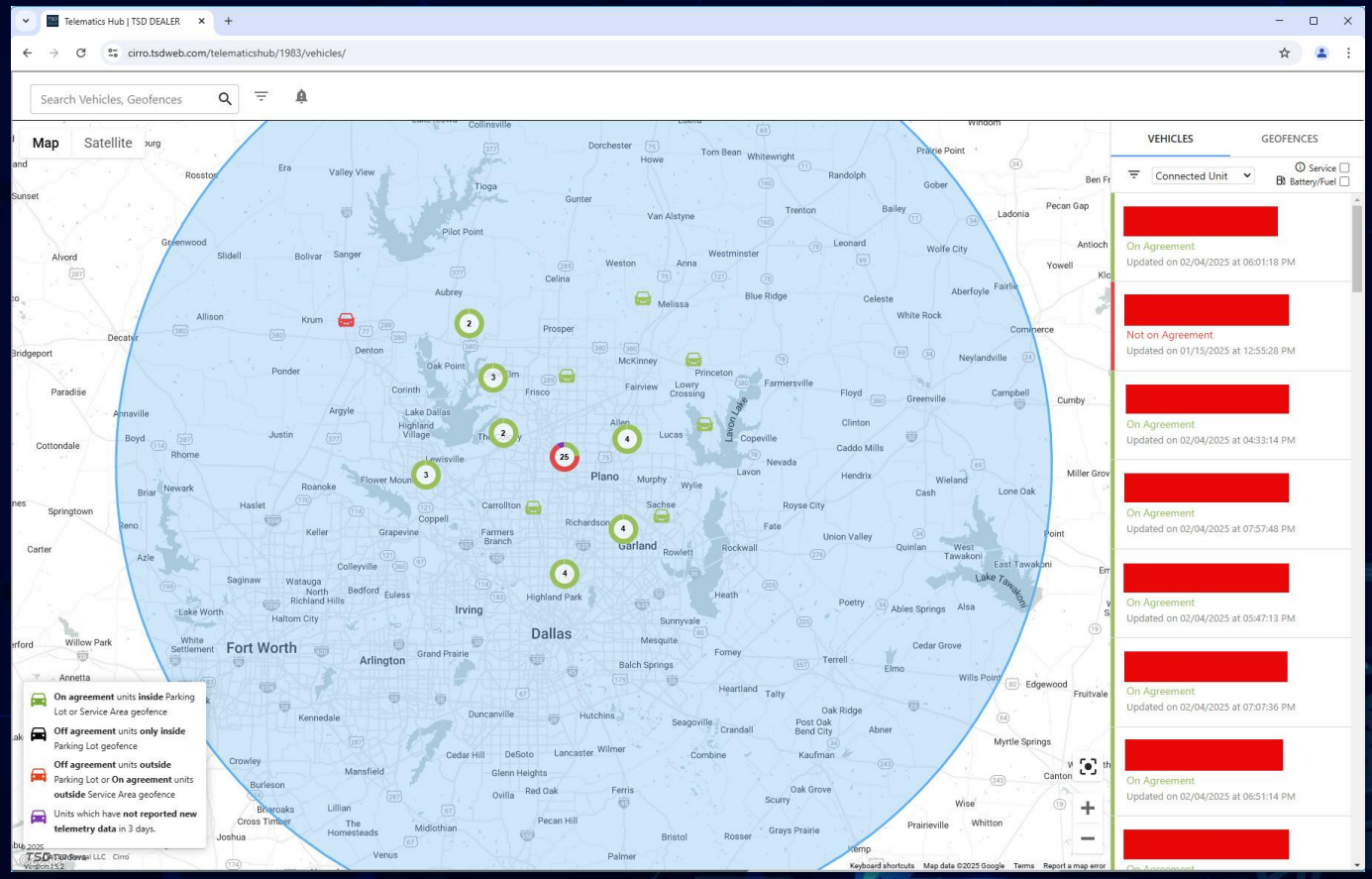


/ TSD Dealer Admin – PII



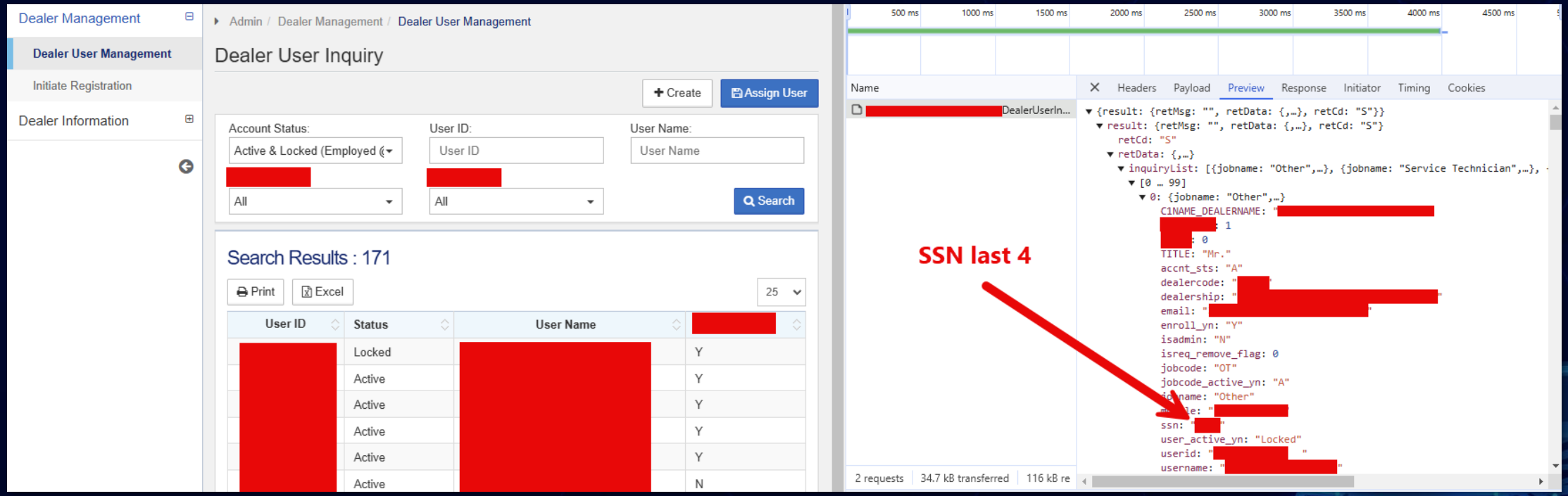
/ TSD Dealer Admin – Connected Cars

- Optional telematics feature
- Real-time fleet tracking
- Prevents theft from customers
  - And geofence to ensure compliance



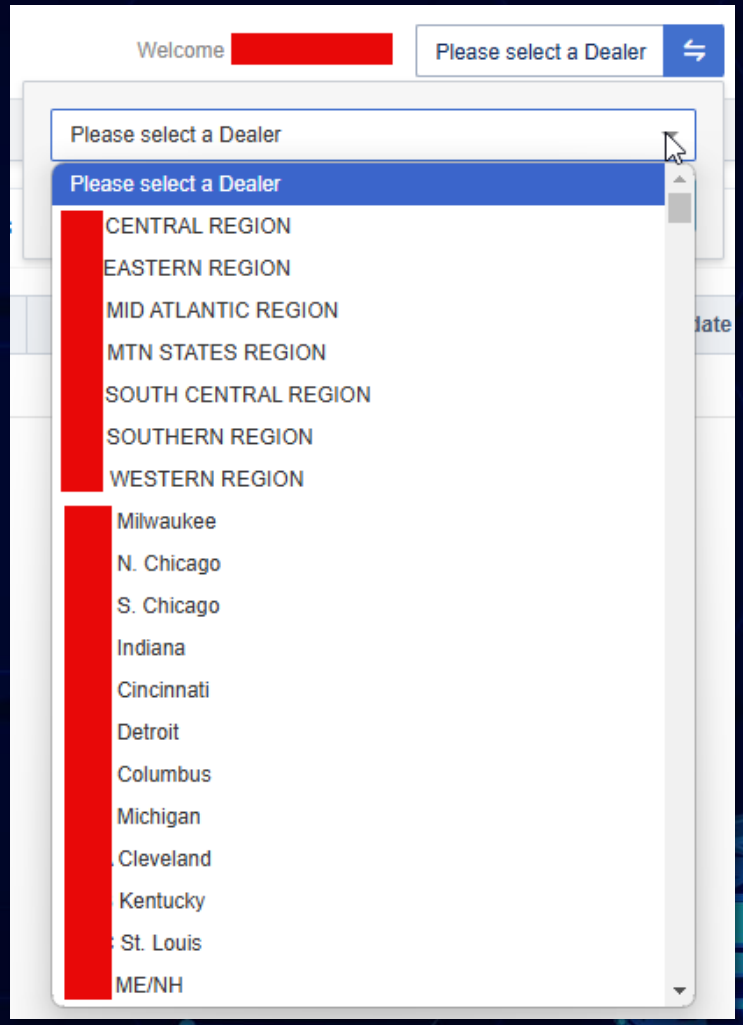
/ Dealer System – Employee PII

- Dealer employee SSN last 4 found in API response
- Option to view full, but would be logged

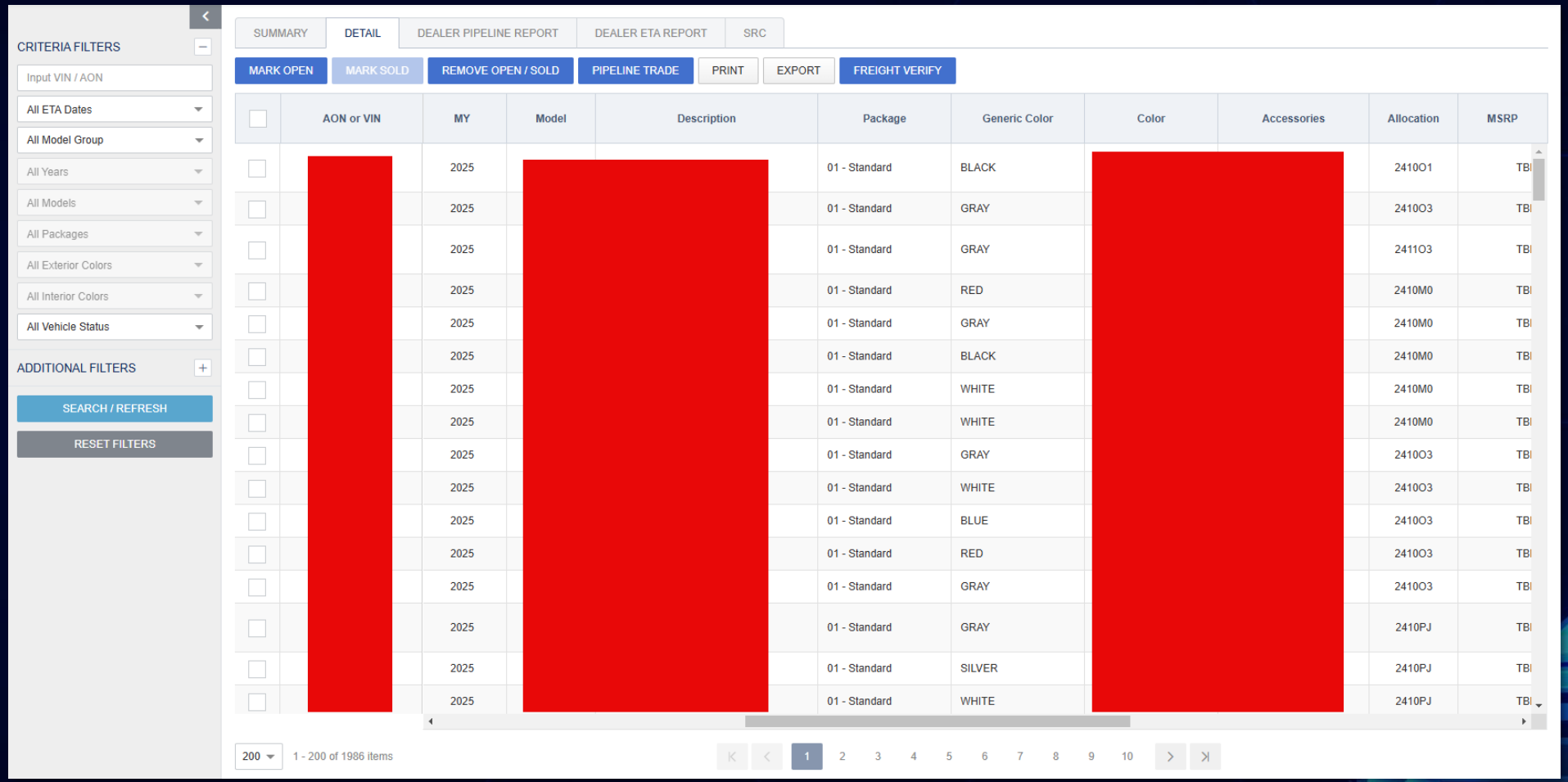


/ Dealer System – Inventory Control

- Dealers have allocation/order tool
- Place orders with HQ, dealer trade
- National admin had total control over it

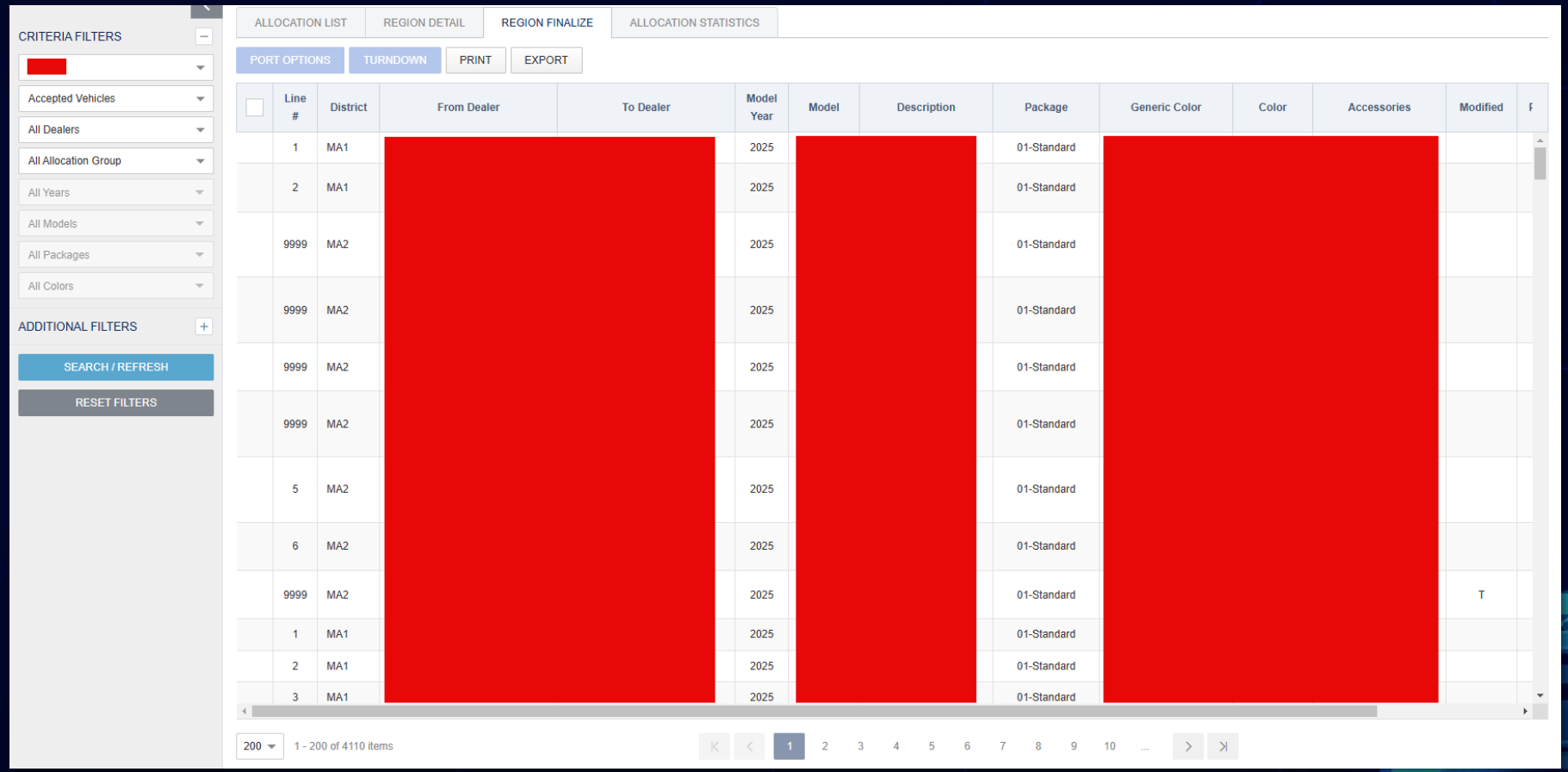


/ Dealer System – Inventory Control Detail

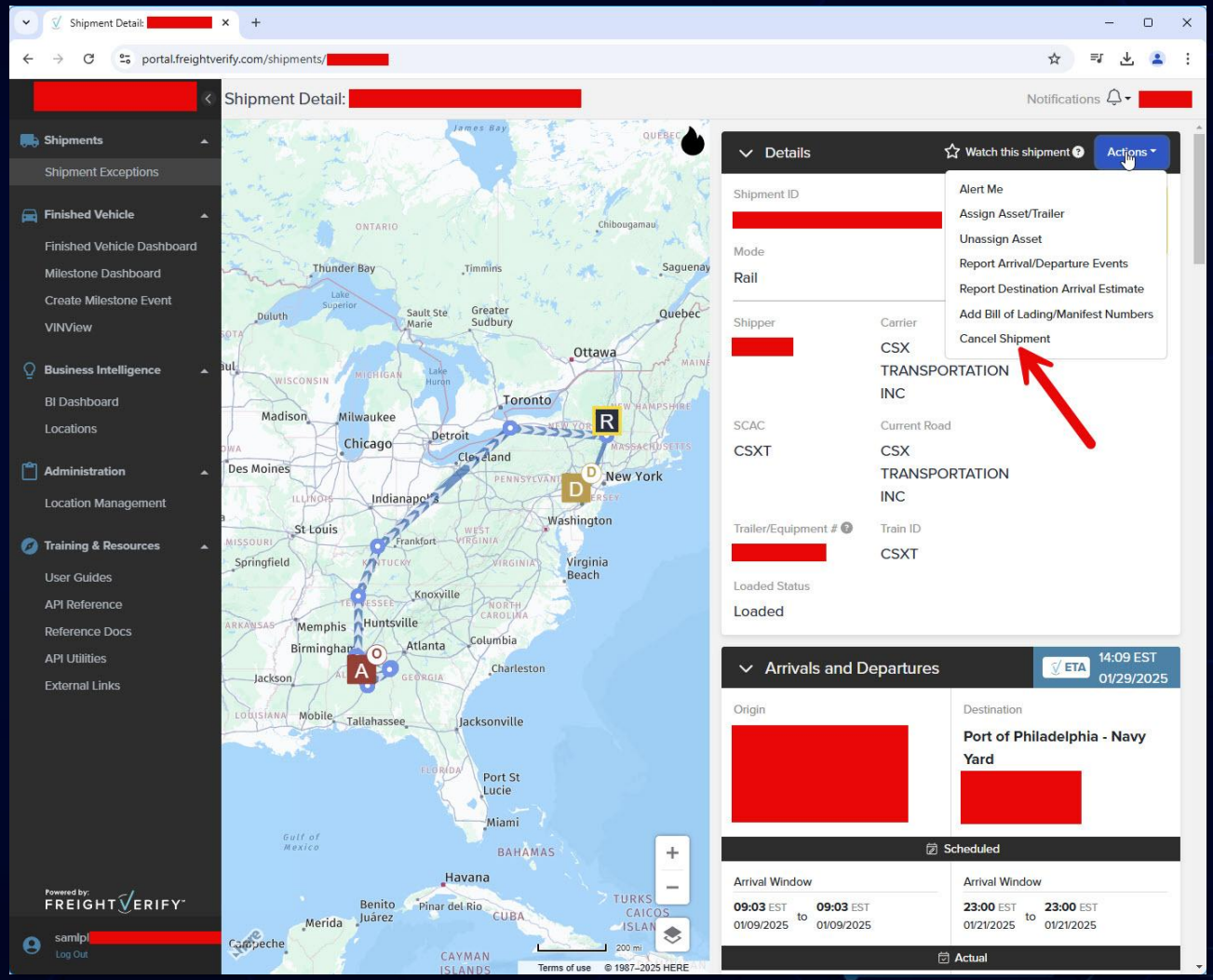


/ Dealer System – Inventory Control (regional)

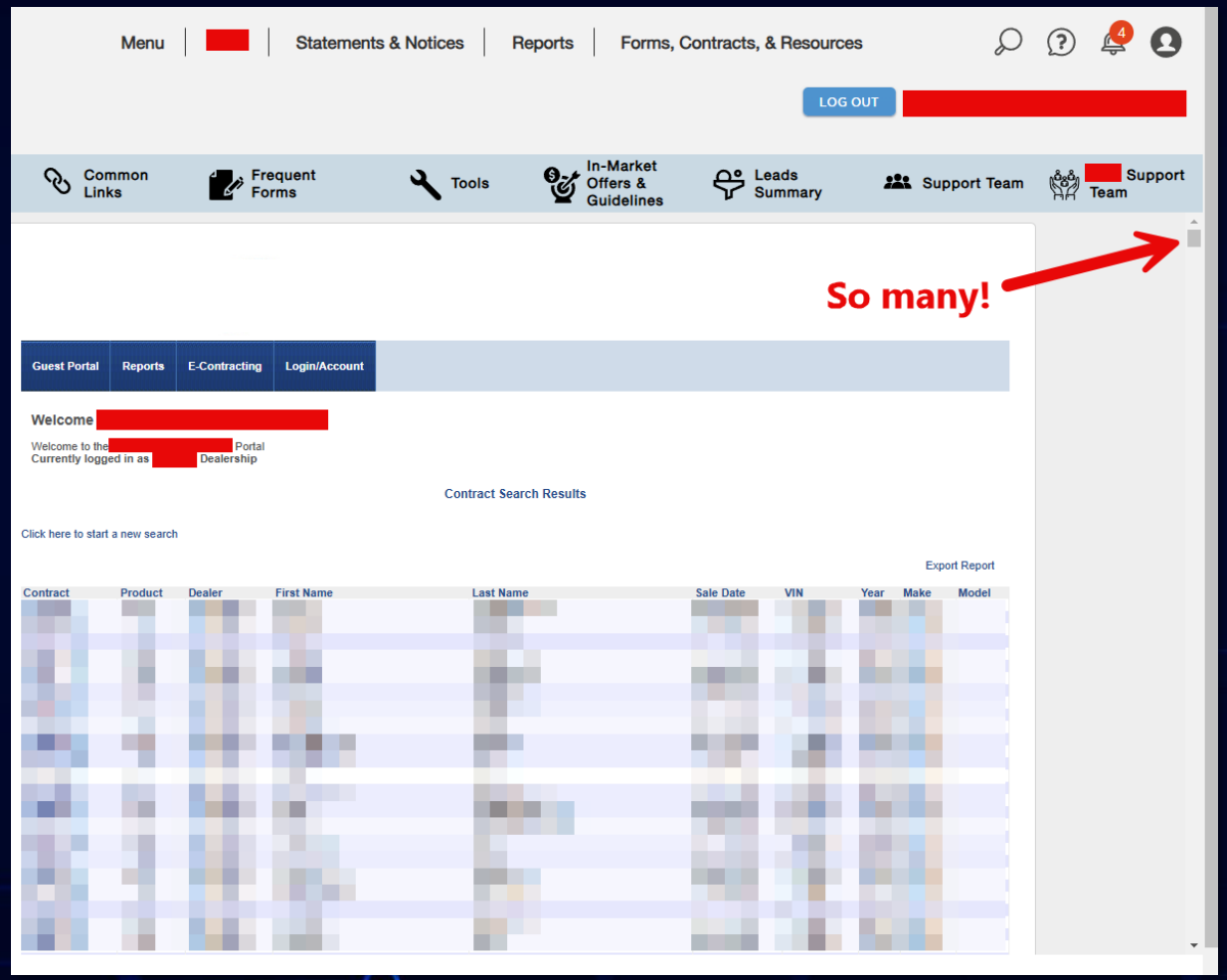
- Special regional access

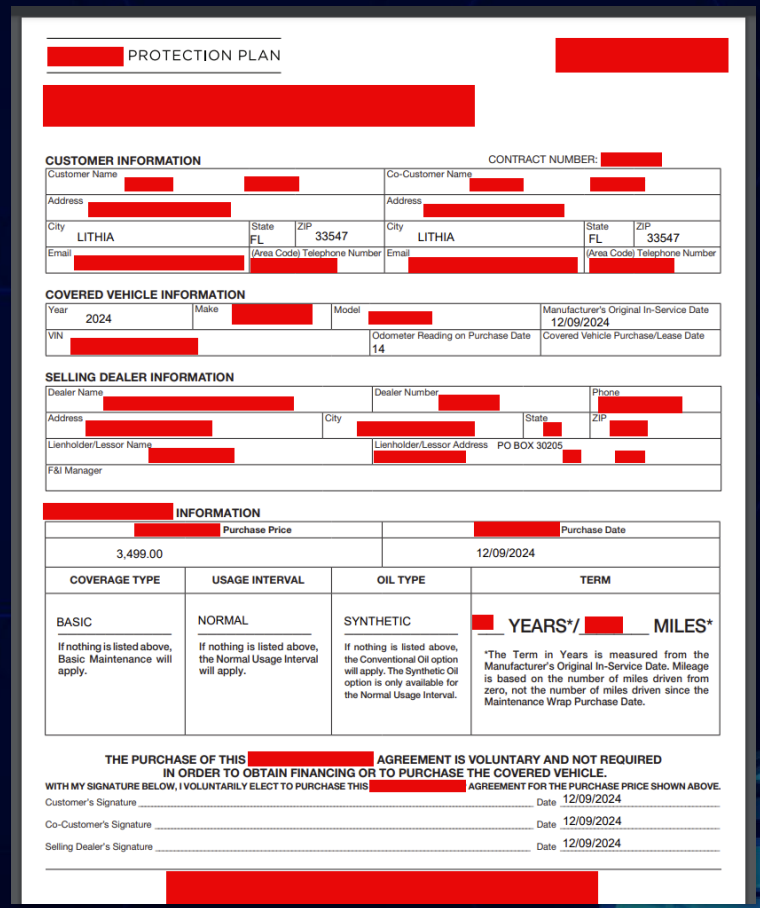


/ FreightVerify – Track & cancel cars

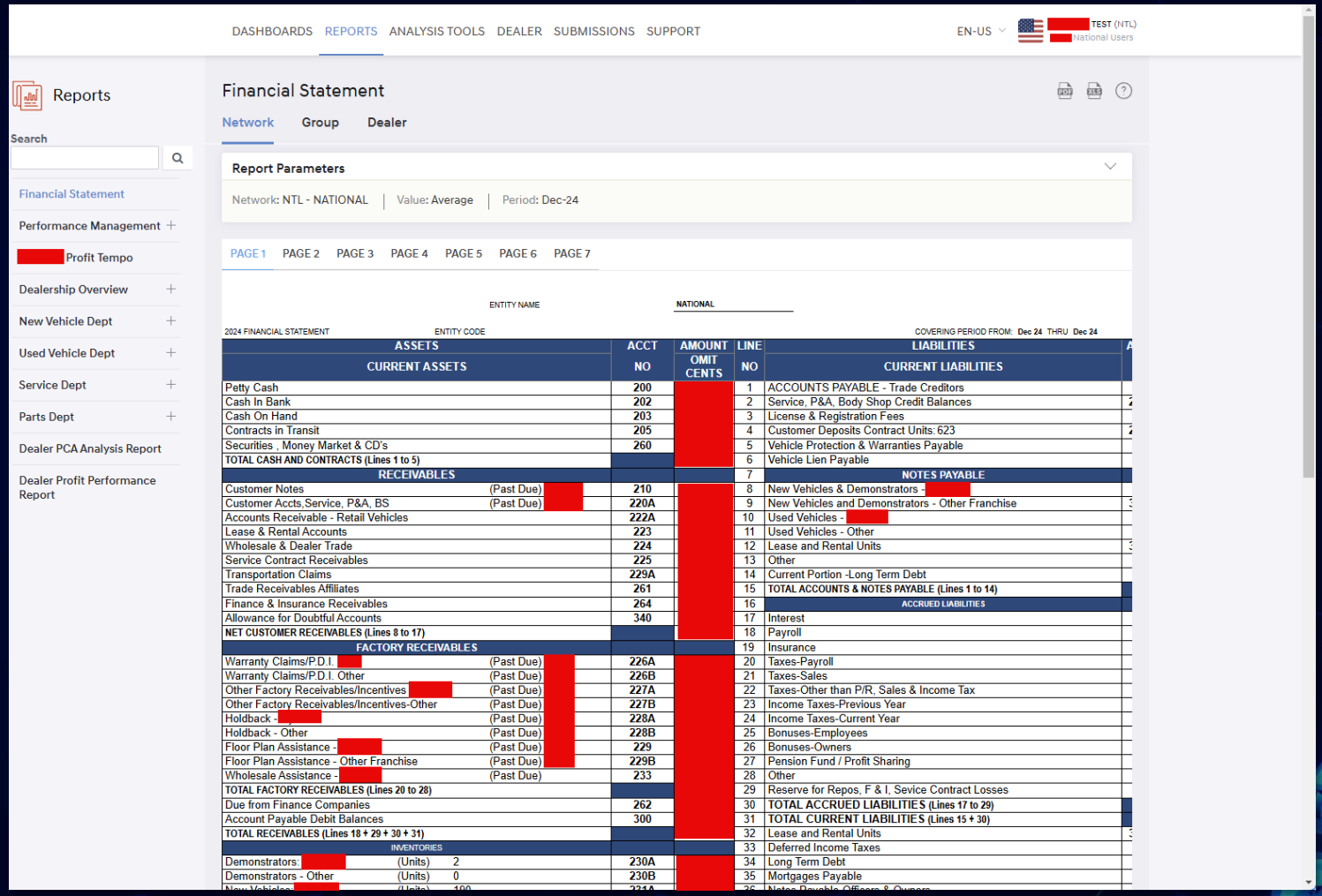


/ Finance Portal





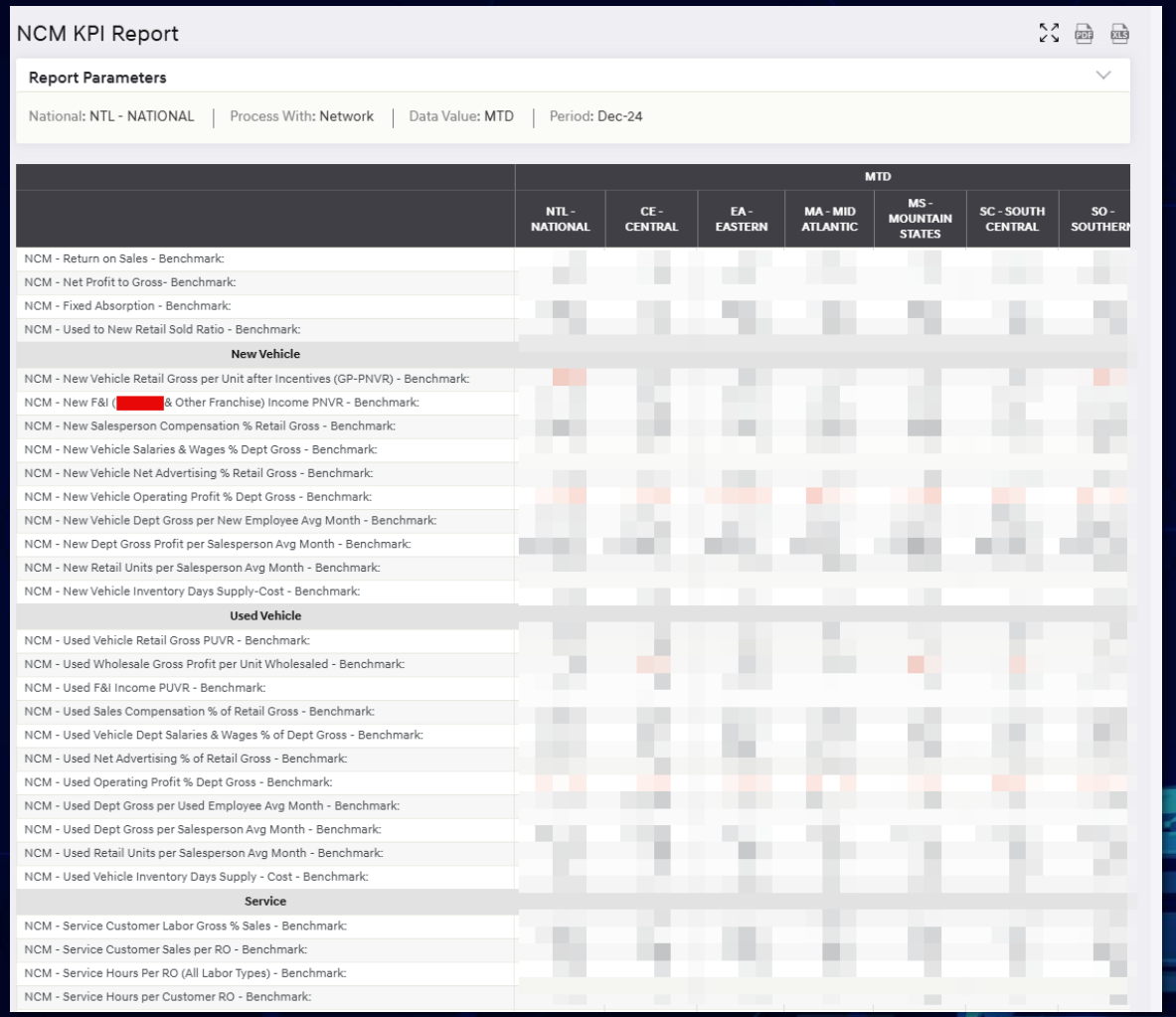
/ Optimum Portal – Finances



ASSETS			ACCT	AMOUNT	LINE	LIABILITIES
CURRENT ASSETS			NO	OMIT CENTS	NO	CURRENT LIABILITIES
Petty Cash			200		1	ACCOUNTS PAYABLE - Trade Creditors
Cash In Bank			202		2	Service, P&A, Body Shop Credit Balances
Cash On Hand			203		3	License & Registration Fees
Contracts in Transit			205		4	Customer Deposits Contract Units: 623
Securities , Money Market & CD's			260		5	Vehicle Protection & Warranties Payable
TOTAL CASH AND CONTRACTS (Lines 1 to 5)					6	Vehicle Lien Payable
RECEIVABLES					7	NOTES PAYABLE
Customer Notes	(Past Due)		210		8	New Vehicles & Demonstrators -
Customer Accts,Service, P&A, BS	(Past Due)		220A		9	New Vehicles and Demonstrators - Other Franchise
Accounts Receivable - Retail Vehicles			222A		10	Used Vehicles -
Lease & Rental Accounts			223		11	Used Vehicles - Other
Wholesale & Dealer Trade			224		12	Lease and Rental Units
Service Contract Receivables			225		13	Other
Transportation Claims			229A		14	Current Portion -Long Term Debt
Trade Receivables Affiliates			261		15	TOTAL ACCOUNTS & NOTES PAYABLE (Lines 1 to 14)
Finance & Insurance Receivables			264		16	ACCRUED LIABILITIES
Allowance for Doubtful Accounts			340		17	Interest
NET CUSTOMER RECEIVABLES (Lines 8 to 17)					18	Payroll
FACTORY RECEIVABLES					19	Insurance
Warranty Claims/P.D.I.	(Past Due)		226A		20	Taxes-Payroll
Warranty Claims/P.D.I. Other	(Past Due)		226B		21	Taxes-Sales
Other Factory Receivables/Incentives	(Past Due)		227A		22	Taxes-Other than P/R, Sales & Income Tax
Other Factory Receivables/Incentives-Other	(Past Due)		227B		23	Income Taxes-Previous Year
Holdback -	(Past Due)		228A		24	Income Taxes-Current Year
Holdback - Other	(Past Due)		228B		25	Bonuses-Employees
Floor Plan Assistance -	(Past Due)		229		26	Bonuses-Owners
Floor Plan Assistance - Other Franchise	(Past Due)		229B		27	Pension Fund / Profit Sharing
Wholesale Assistance -	(Past Due)		233		28	Other
TOTAL FACTORY RECEIVABLES (Lines 20 to 28)					29	Reserve for Repos, F & I, Sevice Contract Losses
Due from Finance Companies			262		30	TOTAL ACCRUED LIABILITIES (Lines 17 to 29)
Account Payable Debit Balances			300		31	TOTAL CURRENT LIABILITIES (Lines 15 + 30)
TOTAL RECEIVABLES (Lines 18 + 29 + 30 + 31)					32	Lease and Rental Units
INVENTORIES					33	Deferred Income Taxes
Demonstrators	(Units)	2	230A		34	Long Term Debt
Demonstrators - Other	(Units)	0	230B		35	Mortgages Payable

/ Optimum Portal – KPIs

- Key Performance Indicator
- Measure of performance



NCM KPI Report

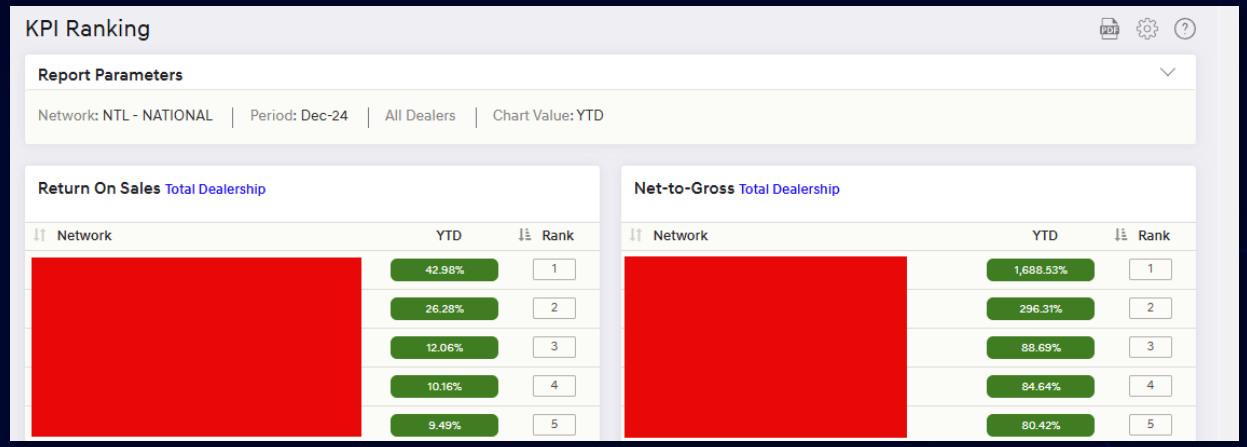
Report Parameters

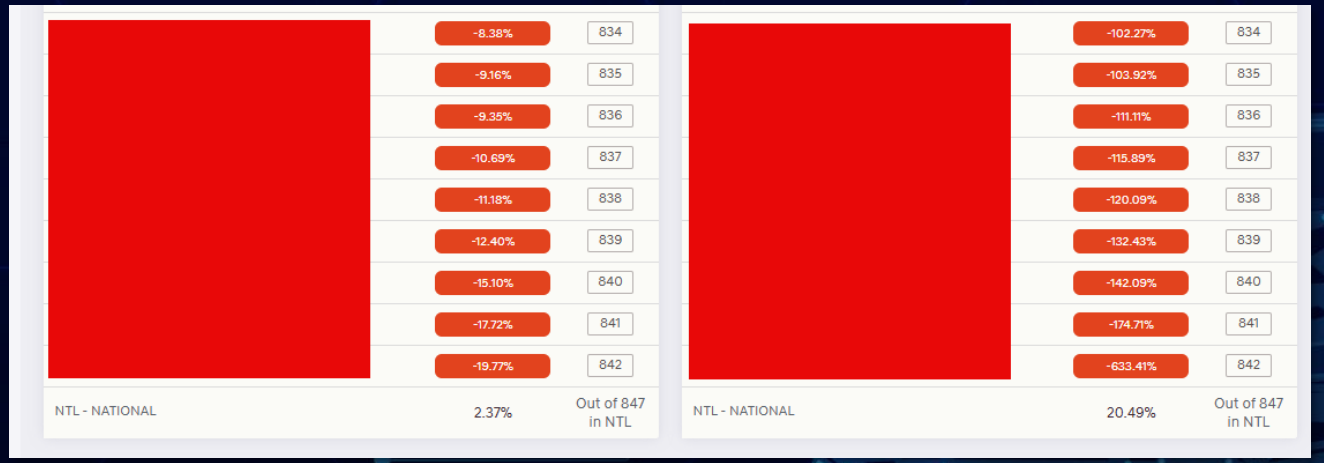
National: NTL - NATIONAL | Process With: Network | Data Value: MTD | Period: Dec-24

	MTD						
	NTL - NATIONAL	CE - CENTRAL	EA - EASTERN	MA - MID ATLANTIC	MS - MOUNTAIN STATES	SC - SOUTH CENTRAL	SO - SOUTHERN
NCM - Return on Sales - Benchmark:							
NCM - Net Profit to Gross- Benchmark:							
NCM - Fixed Absorption - Benchmark:							
NCM - Used to New Retail Sold Ratio - Benchmark:							
New Vehicle							
NCM - New Vehicle Retail Gross per Unit after Incentives (GP-PNVR) - Benchmark:							
NCM - New F&I (& Other Franchise) Income PNVR - Benchmark:							
NCM - New Salesperson Compensation % Retail Gross - Benchmark:							
NCM - New Vehicle Salaries & Wages % Dept Gross - Benchmark:							
NCM - New Vehicle Net Advertising % Retail Gross - Benchmark:							
NCM - New Vehicle Operating Profit % Dept Gross - Benchmark:							
NCM - New Vehicle Dept Gross per New Employee Avg Month - Benchmark:							
NCM - New Dept Gross Profit per Salesperson Avg Month - Benchmark:							
NCM - New Retail Units per Salesperson Avg Month - Benchmark:							
NCM - New Vehicle Inventory Days Supply-Cost - Benchmark:							
Used Vehicle							
NCM - Used Vehicle Retail Gross PUVR - Benchmark:							
NCM - Used Wholesale Gross Profit per Unit Wholesaled - Benchmark:							
NCM - Used F&I Income PUVR - Benchmark:							
NCM - Used Sales Compensation % of Retail Gross - Benchmark:							
NCM - Used Vehicle Dept Salaries & Wages % of Dept Gross - Benchmark:							
NCM - Used Net Advertising % of Retail Gross - Benchmark:							
NCM - Used Operating Profit % Dept Gross - Benchmark:							
NCM - Used Dept Gross per Used Employee Avg Month - Benchmark:							
NCM - Used Dept Gross per Salesperson Avg Month - Benchmark:							
NCM - Used Retail Units per Salesperson Avg Month - Benchmark:							
NCM - Used Vehicle Inventory Days Supply - Cost - Benchmark:							
Service							
NCM - Service Customer Labor Gross % Sales - Benchmark:							
NCM - Service Customer Sales per RO - Benchmark:							
NCM - Service Hours Per RO (All Labor Types) - Benchmark:							
NCM - Service Hours per Customer RO - Benchmark:							

/ Optimum Portal – Dealer Rankings

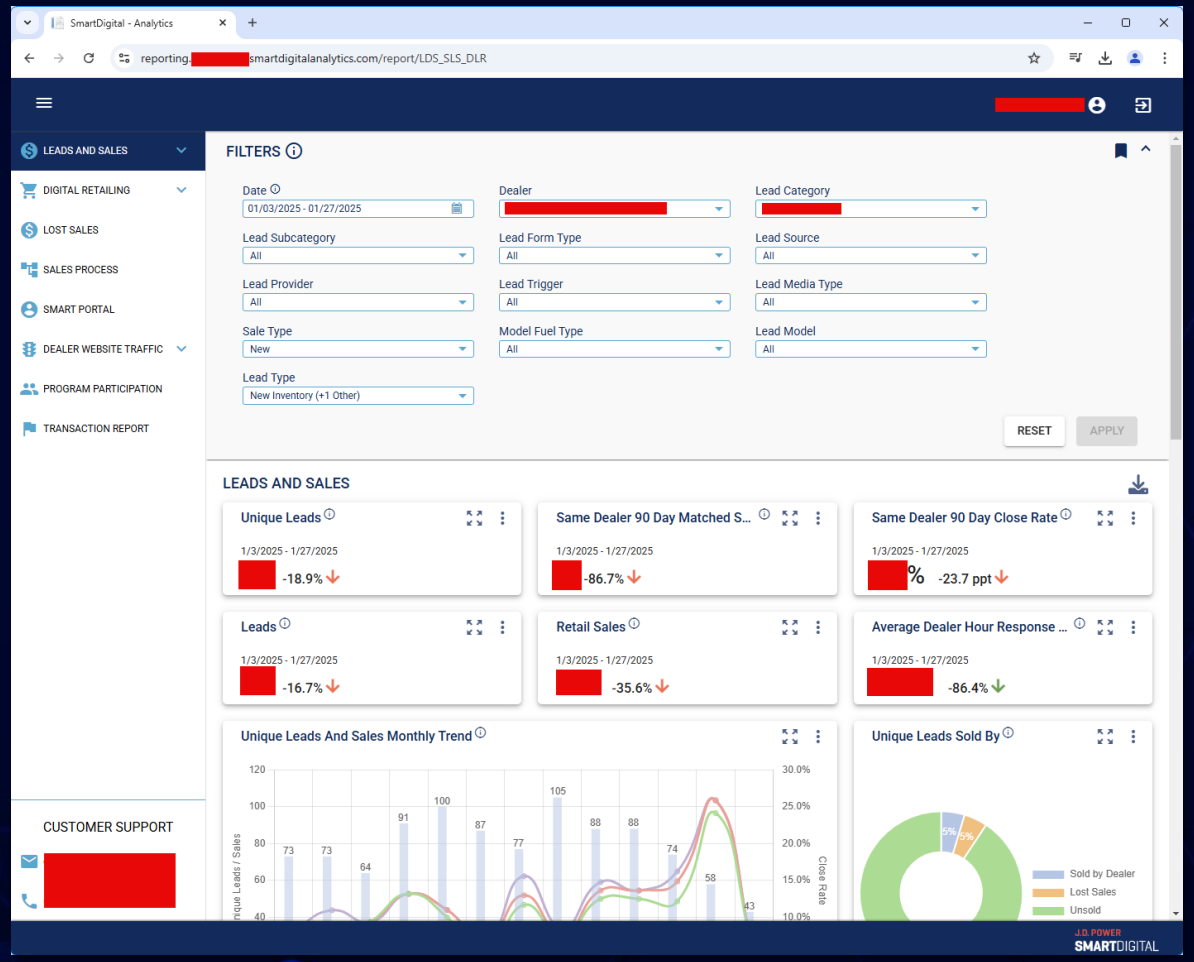
- Ever wanted to know the real good/bad dealers?

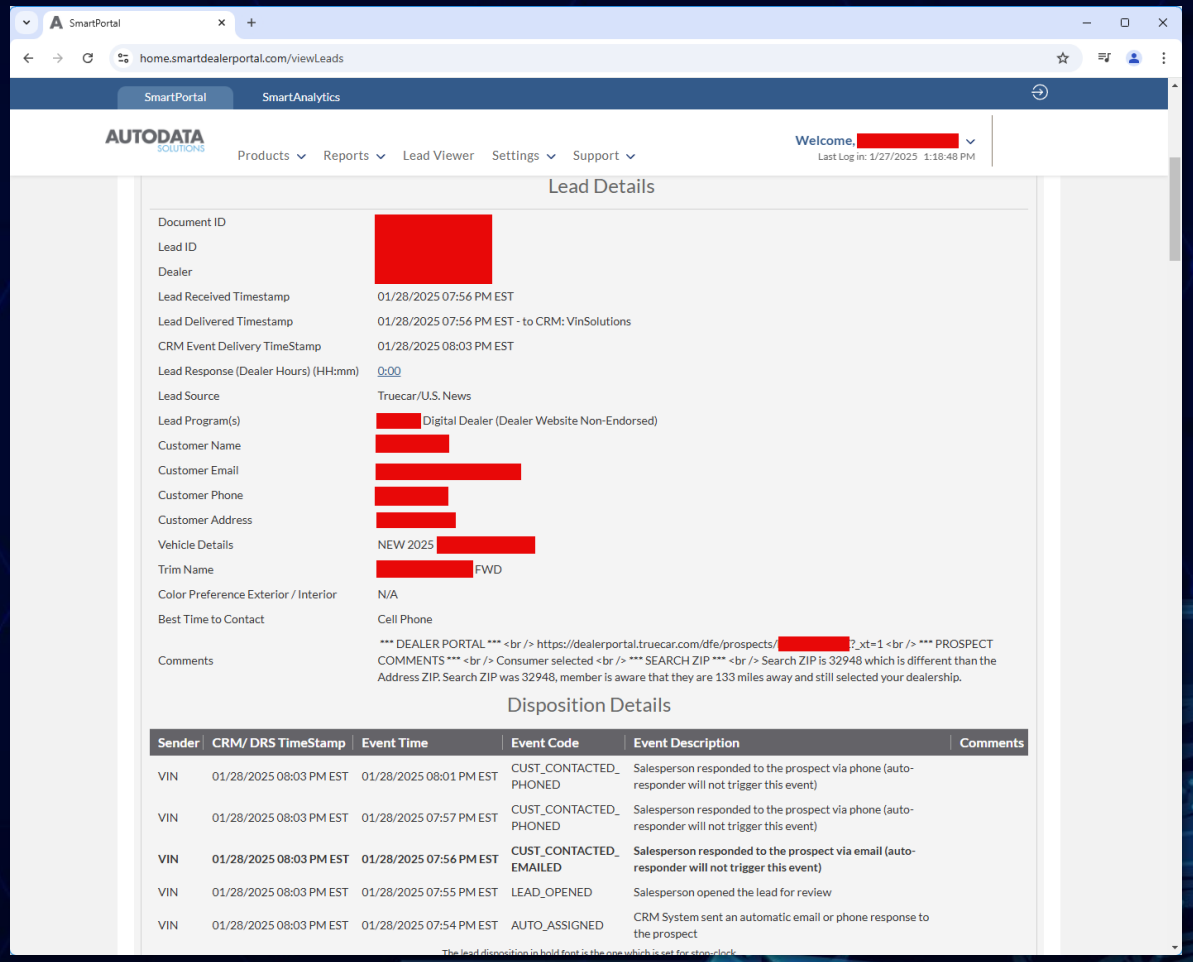




/ J.D. Power Portals

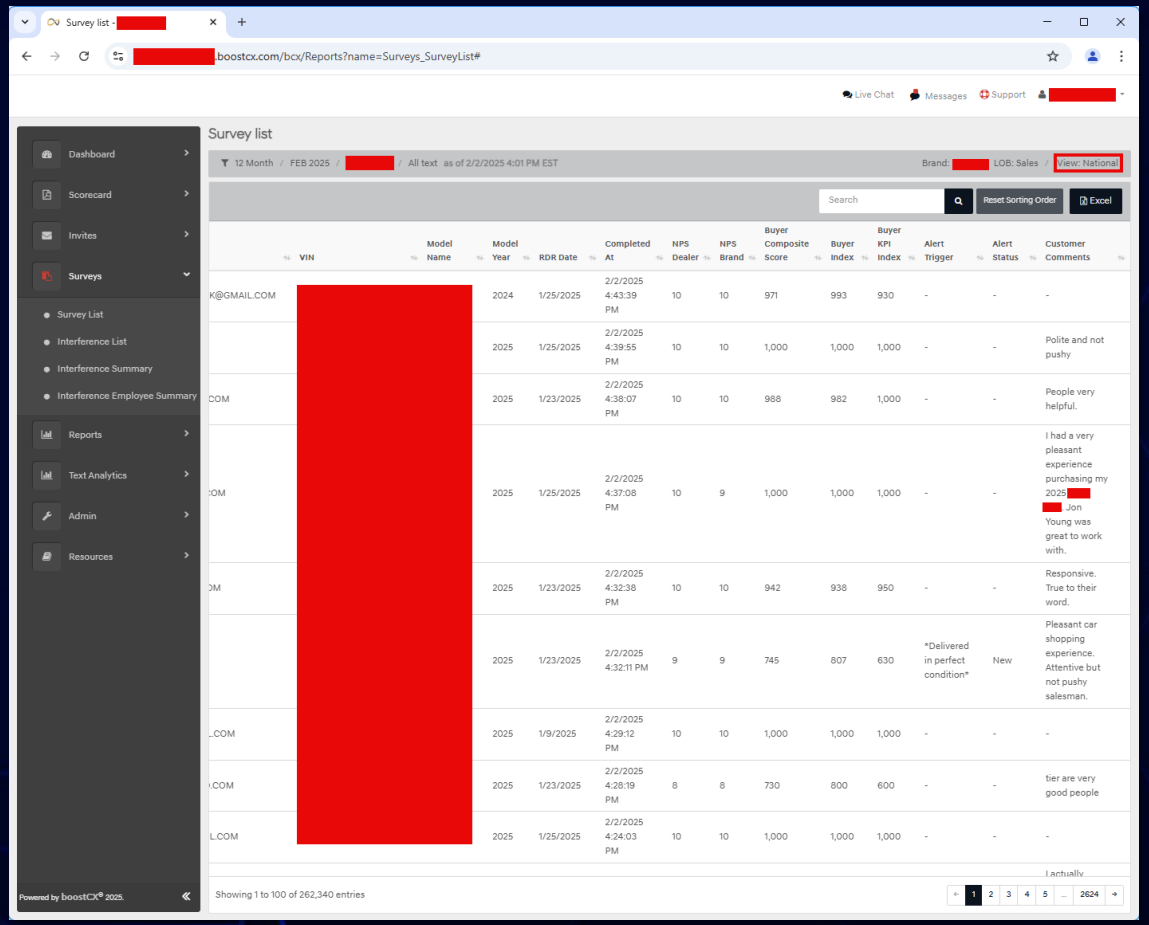
- For analytics, sales

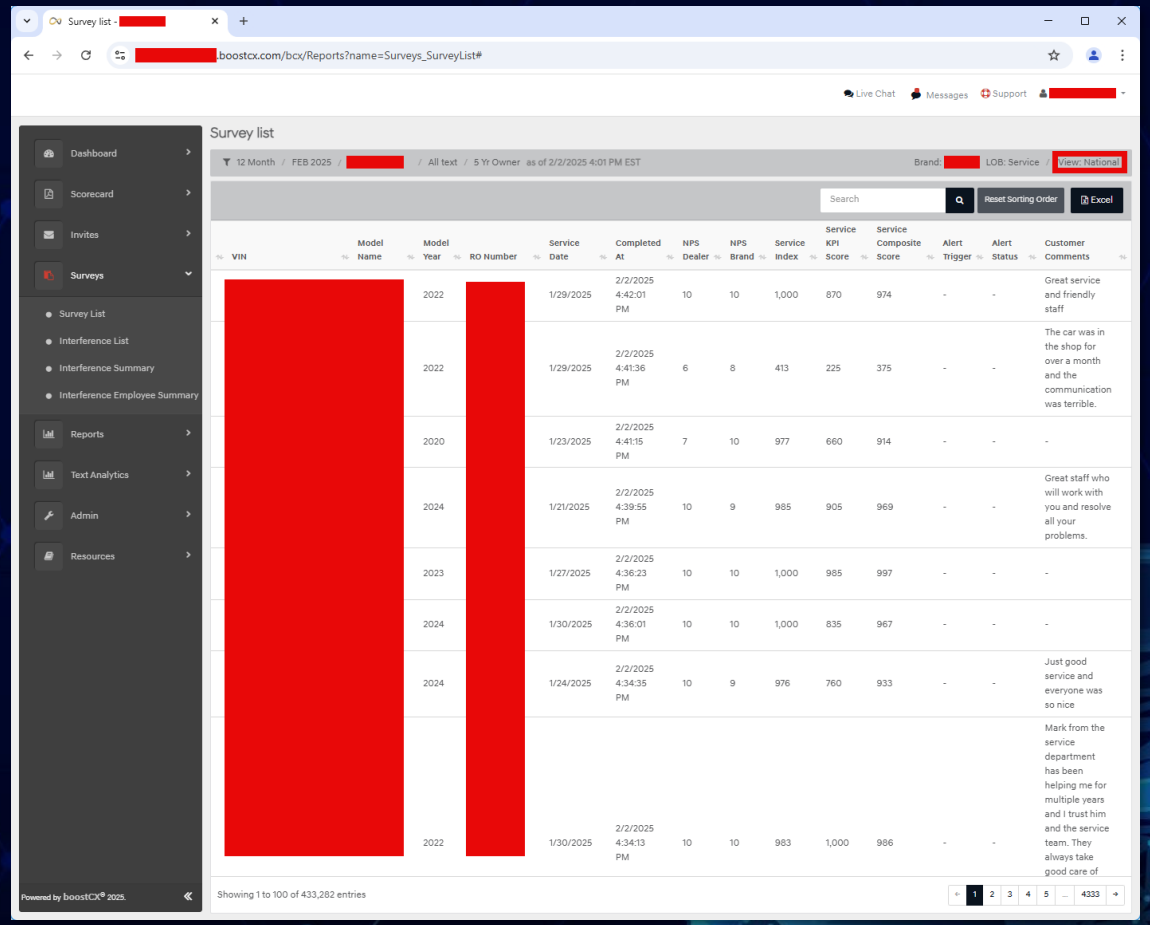




/ boostCX Surveys

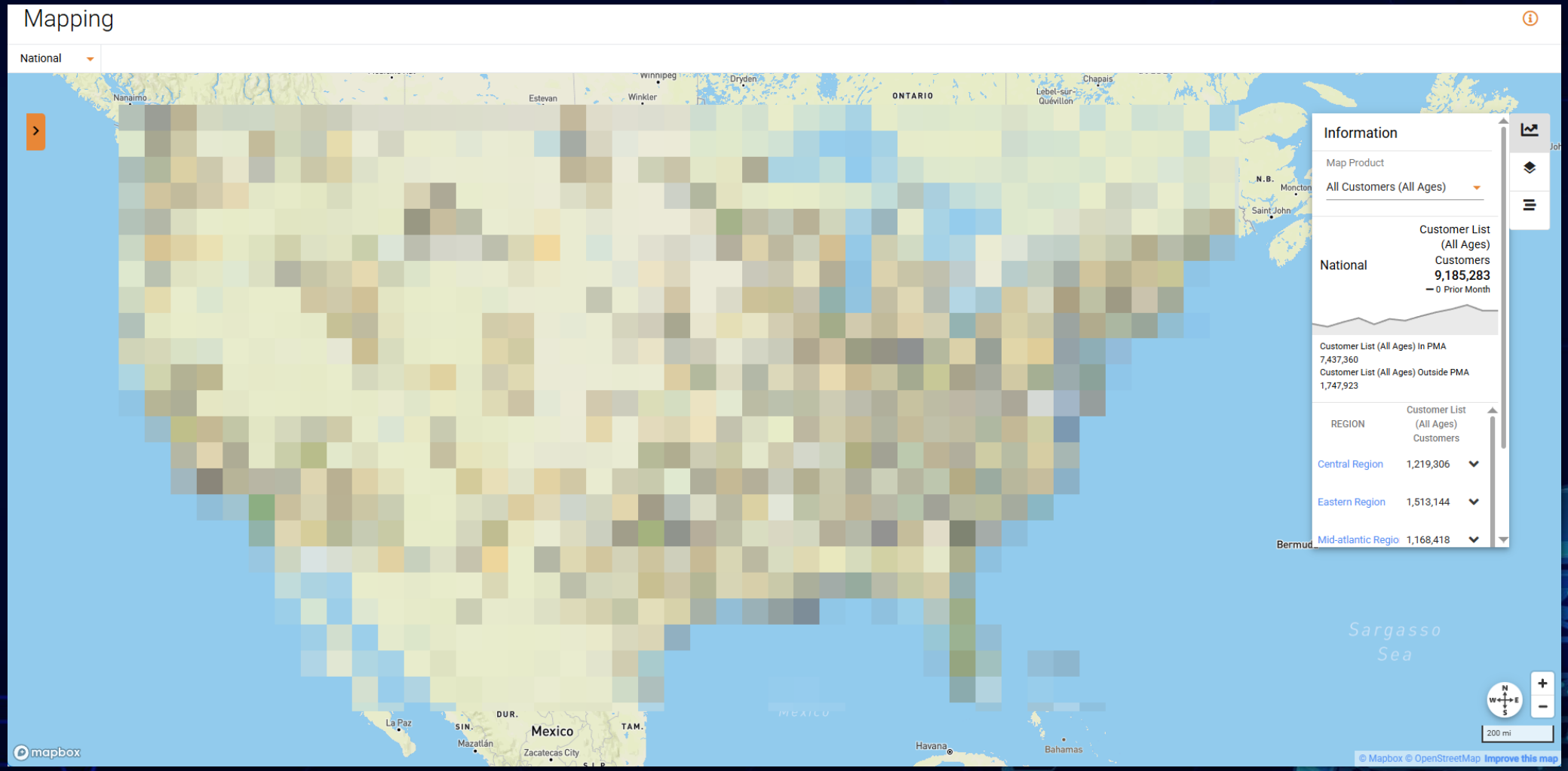
- Those surveys we all love. Want to see what your friend really thinks of their car? I could find out!





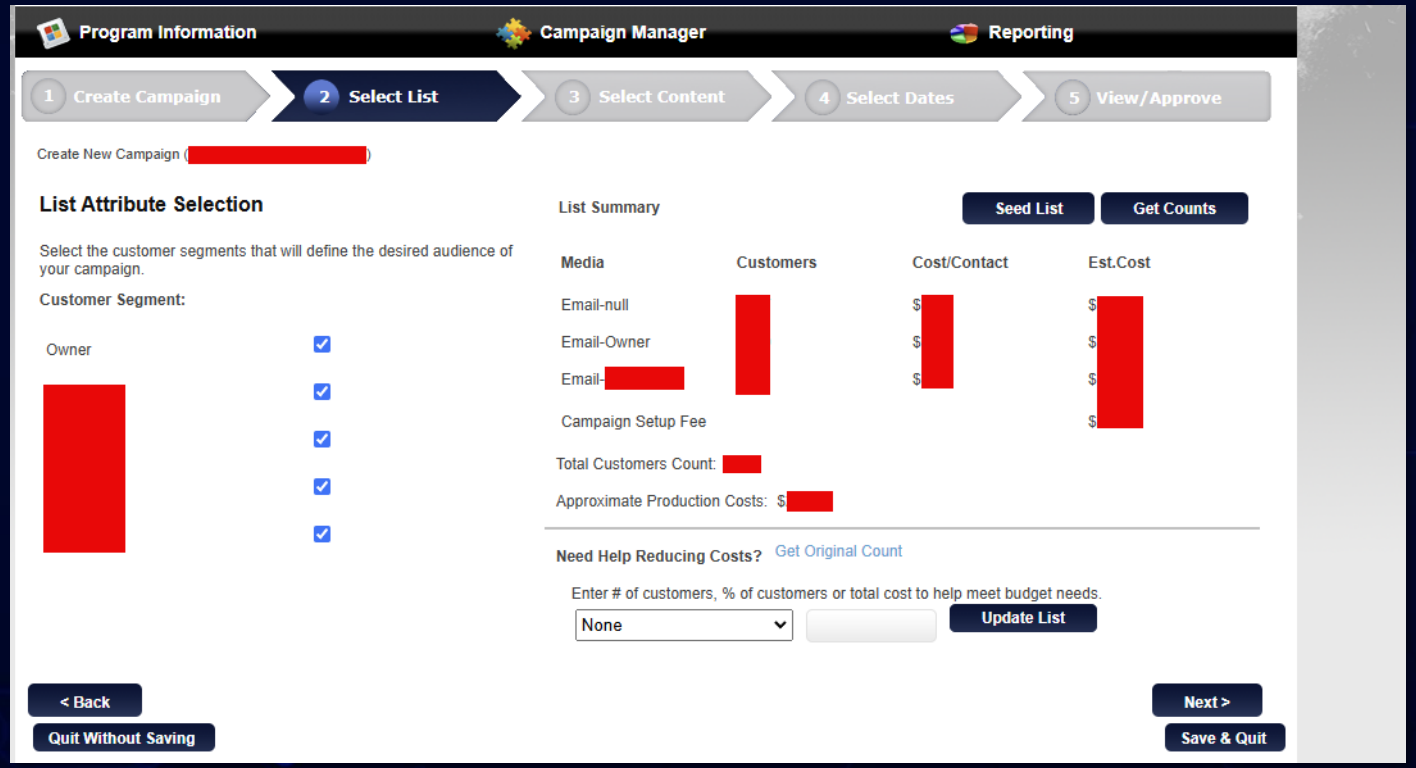
/ Aftersales map for growth

Over 9 million people!



/ Phishing on the dealer's dime

- Marketing platform exists for mail & email
- Ability to create campaign using dealer customer base, bill them for it





/ Disclosure Timeline

- **Jan 26, 2025:** Discovered. Spent about a week exploring, undetected. Very careful to limit actions to read-only.
- **Feb 3, 2025:** Reported through VDP.
- **Feb 6, 2025:** Response received confirming they are investigating.
- **Feb 11, 2025:** Response received confirming fixes, verified.
- **Feb 12, 2025 onward:** Continued collaboration & meetings with vendor to answer questions and coordinate this disclosure.
- **DEF CON 33:** Public disclosure / world premiere.



/ Final Takeaways

- Dealer systems powerful, loaded with your personal info
- Dealer systems more interconnected than ever. Rogue employee = critical impacts
- Simple flaws can have devastating effects on them and YOU
- Even more potential, but had to stop & report eventually
- That’s all! Now go rip out your headunits 🛠️



linkedin.com/in/eatonz/



eaton-works.com

EATON WORKS

harness