

COMPLYAUTO 



Navigating Compliance: Essential Updates & Best Practices for Cybersecurity

September 26, 2024



Legal Disclaimer

This presentation is intended to be used as a compliance aid. Reasonable efforts have been made to ensure the accuracy and completeness of the following subject matter. No express or implied warranty is provided respecting the information contained in this presentation. The following material should not be construed as (nor used as a substitute for) legal advice. If legal advice is required, the services of a competent professional should be sought. Each dealer must rely on its own expertise and knowledge of law when using the material provided.

This webinar, and your participation in the webinar, may be monitored, recorded, and shared.

This presentation is the property of ComplyAuto Privacy LLC. All rights reserved. Copyright 2024. Not to be distributed without consent of ComplyAuto.

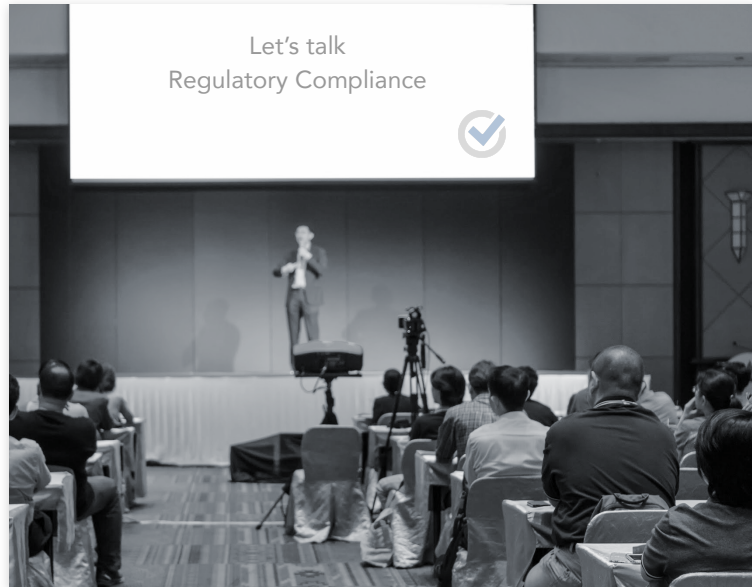
Who We Are

ComplyAuto is transforming regulatory compliance

- 10,000+ active dealers across all 50 states
- 40+ dealer association endorsements

FOR DEALERS. BY DEALERS.

We were founded by compliance experts, lawyers, and principals with decades of experience running dealerships. We are your strategic partners in all things regulatory and all things compliance.



1/4 of our entire staff are former dealership employees and **even more** have worked in the automotive industry

COMPLYAUTO 

ComplyAuto has the most lawyers and compliance experts



Chris Cleveland
Co-Founder & CEO



Brad Miller
Chief Compliance/ Regulatory Officer
Head of Legal



Talar Coursey
General Counsel
& VP of Legal Product



Hao Nguyen
Senior Product &
Regulatory Counsel



Andy Graff
Chief Operating Officer



Nick Moyes
Strategic Partnerships &
Regulatory Compliance Manager



Mark Sanborn
Senior Product &
Regulatory Counsel

Data Breach - Now What?



CDK Cyber Incident

→ BACKGROUND/OVERVIEW

→ 8/26/24 Update from CDK:

“We are pleased to report that after conducting a thorough third-party expert review **we have not discovered a compromise** of dealer, dealer employee, or consumer personally identifiable information **that would give rise to any notification obligations** relating to the incident.

While we made a commitment to file consolidated notices on behalf of dealers, under federal or other privacy laws, our findings confirm that no filings are necessary.”

But see Safeguards Rule: - Unauthorized acquisition will be presumed to include unauthorized access to unencrypted customer information unless you have reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of such information.

Safeguards Overview

Safeguards rule finalized June 9th 2023. No enforcement yet...but

New FTC reporting requirement became effective May 13, 2024.

Reminder: Ongoing Requirements:

- Annual Board Report
- Risk Assessments
- Penetration Tests and Vulnerability Scans
- Employee Training
- Phishing
- ComplyAuto resources available

Data Security - Bottom Line: Don't get breached!



No way to be 100% sure, but there are steps you:

1. Must take
2. Should take

What should dealers do now?

- Ensure complete Safeguards Compliance
 - ◆ First step in any claim: “Show me your Safeguards materials”
 - ◆ Update as required in the wake of an “incident”
 - Vendor review
 - Information Security Program Update
 - Board report - Annual Reporting Requirement
 - ◆ Vendor “audits”
 - ◆ ComplyAuto has most complete suite of tools available to dealers.
- Review contracts and be prepared
 - ◆ Safeguards compliance
 - ◆ Breach notification obligations
 - ◆ Indemnification
 - ◆ Data Security representations
- Cybersecurity Insurance

Limiting Potential Liability



What should dealers do now?

Technical Mitigation Steps

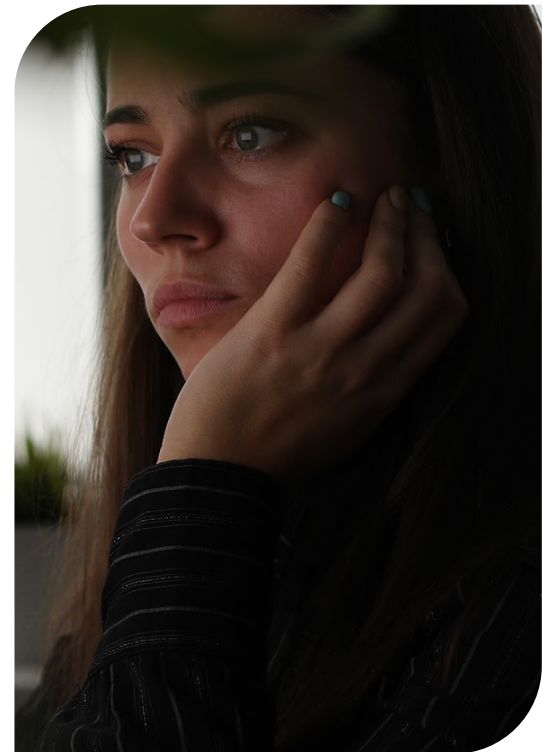
- **Remediate Vulnerabilities:** Perform penetration testing, vulnerability scans, and regularly update and patch systems.
- **User Training:** Train employees to recognize and report phishing.

NOTE: [ComplyAuto has CDK-specific phishing template available now](#)

- **Authentication:** Enforce multi factor authentication (MFA) and use strong, unique passwords.
- **Network Security:** Segment networks, disable unused ports, and apply least privilege (PoLP).
- **Backups:** Maintain encrypted, offline backups and regularly test restoration.
- **Detection & Response:** Use endpoint detection and response (EDR) tools, monitor network traffic (DLP), and update antivirus software.
- **Additional Measures:** Disable command-line activities and add email banners for external emails. Use email security tools and automated spam/phishing filters.

Breach Reporting Requirements

- Dealers (as financial institutions subject to GLBA) must report certain breach-related events to the FTC
- “Notification Event” - “acquisition of unencrypted customer information without the authorization of the individual to which the information pertains.”
- Notification required if event involves
 - ◆ Customer Information (contains NPI)
 - ◆ 500 or more customers
 - ◆ Unencrypted



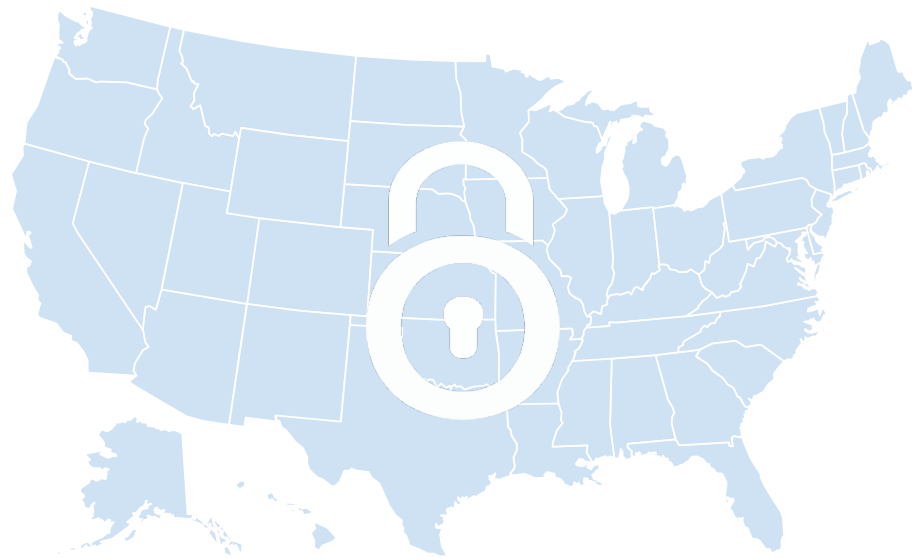
Reports must be made



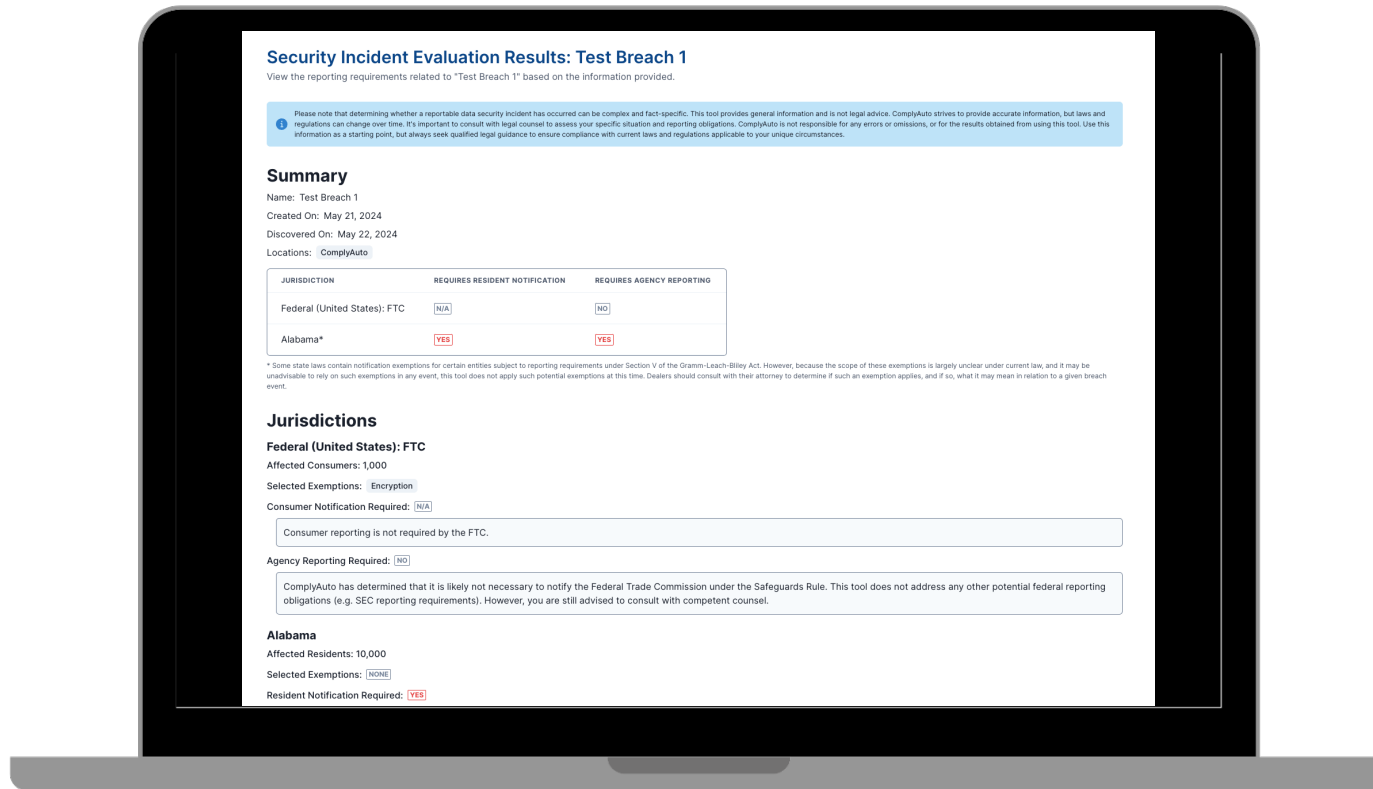
- Using a [form](#) on the FTC Website
- “As soon as possible and no later than 30 days after discovery”
 - ◆ Discovery = the first day you (your employees or agents) become aware
 - ◆ Does the breach involve any vendors?
- Exceptions if law enforcement is involved

State Data Breach Laws

- All 50 States have reporting requirements
- Important to understand the difference with the FTC requirement, potential overlap
- Each state has their own requirements
- Generally also only applies to certain types of sensitive and **encrypted** information



New Breach Notification and Reporting Evaluation Tool



Sample Breach Notification Template

Appendix A: Sample Data Breach Notification Letter

ComplyAuto, Date: *[Insert Date]*

NOTICE OF DATA BREACH

Dear *[Insert Name]*:

We are contacting you about a data breach that has occurred at ComplyAuto

What Happened?

[Describe how the data breach happened, the date of the breach, and how the stolen information has been misused (if you know)].

What Information Was Involved?

This incident involved your *[describe the type of personal information that may have been exposed due to the breach]*.

What We Are Doing

[Describe how you are responding to the data breach, including: what actions you've taken to remedy the situation; what steps you are taking to protect individuals whose information has been breached; and what services you are offering (like credit monitoring or identity theft restoration services)].

What You Can Do

[Insert the following language if the information compromised poses a high risk of identity theft or social security numbers were compromised].

The Federal Trade Commission (FTC) recommends that you place a free fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Contact any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for one year. You can renew it after one year.

Equifax: equifax.com/personal/credit-report-services or 1-800-685-1111

Experian: experian.com/help or 1-888-397-3742

TransUnion: transunion.com/credit-help or 1-888-909-8872

Ask each credit bureau to send you a free credit report after it places a fraud alert on your file. Review your credit reports for accounts and inquiries you don't recognize. These can be signs of identity theft. If your personal information has been misused, visit the FTC's site at identitytheft.gov to report the identity theft and get recovery steps. Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit reports periodically so you can spot problems and address them quickly.

You may also want to consider placing a free credit freeze. A credit freeze means potential creditors cannot get your credit report. That makes it less likely that an identity thief can open new accounts

in your name. To place a freeze, contact each of the major credit bureaus at the links or phone numbers above. A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it.

[Insert the following language if you choose to provide a copy of the FTC's identity theft guide].

We have attached information from the FTC's website, identitytheft.gov/databreach, about steps you can take to help protect yourself from identity theft. The steps are based on the types of information exposed in this breach.

Other Important Information

[Insert other important information here]

For More Information

Call *[telephone number]* or go to *[Internet website]*. *[State how additional information or updates will be shared/or where they will be posted].*

[Insert Closing]

[Your Name]

Cookie Consent and Online Privacy Updates



Cookies and Tracking Technologies - Overview



- Over the past few months, there has been a surge in lawsuits related to online tracking tech. Dealers are one of the latest industry targets, along with OEMs, website providers, and other automotive vendors.
- These claims have not been widely reported largely because the overwhelming majority settle before being publicized.
- Claims allege wiretapping and similar privacy violations in connection with common website tracking technologies like cookies, Google Analytics, Meta Pixel, and website chat modules.
- The merits of the arguments are often dubious, but the courts are currently split on how to handle these cases, and defending or settling these cases can be very expensive (similar to ADA cases).

19 States with Privacy Laws

Dealers can't ignore Privacy laws or Cookie Consent

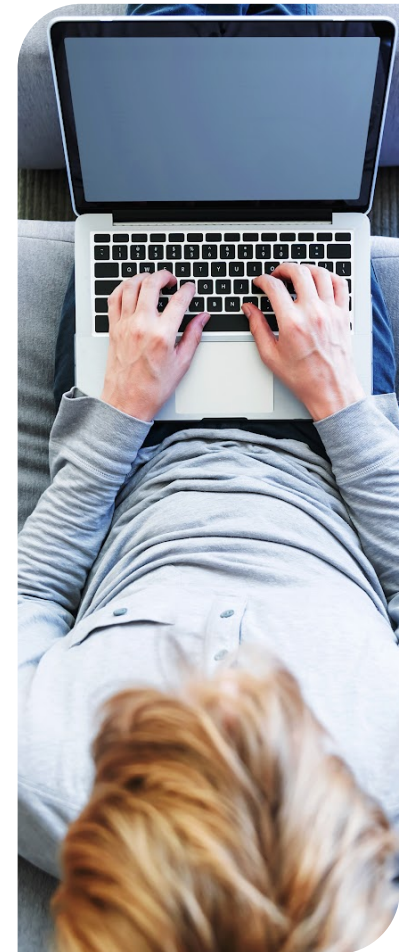
Some states include

Consumer Rights

- Right to know
- Right to correct
- Right to delete
- Right to opt out of target ads
- Right to portability

Business Obligations

- Opt-in default of sensitive data
- Notice/transparency requirement
- Risk assessments
- Prohibition exercising rights
- Purpose/processing limitation
- Does not have an entity level exemption for GLBA only exempts GLBA data





Similar Allegations & Enforcement Actions

1. Federal Wiretapping
2. FTC Act Section 5 (UDAP)
3. "Pen Register" Surveillance
(more than 50 lawsuits filed recently)
4. Recording Communications without all parties' consent
5. State Privacy Laws

“Wiretapping Claims”

Since 2023, there have been hundreds of lawsuits filed against retailers and other businesses (including third-party service providers). It’s increasing in 2024.

- RODRIGUEZ v. FORD MOTOR CO.
- JESSE CANTU v. DEALER DOT COM, INC.
- SANTORO V. HYUNDAI MOTOR AMERICA
- D’ANGELO v. FCA US, LLC d/b/a DODGE
- SANCHEZ V. CARS.COM INC.
- RODRIGUEZ V. AUTOTRADER.COM
- KIRKHAM v. TAXACT
- MONICA SANCHEZ V. CARGURUS, INC.
- RODRIGUEZ V. AVIS RENT A CAR SYSTEMS
- RODRIGUEZ V. JAGUAR LAND ROVER NORTH AMERICA
- HASSON v. PARTS ID
- HUFF v. INTERNET TRUCKSTOP GROUP

Claims generally focus on the following:

- Violation of state wiretapping laws (eavesdropping on website activity & communications without consent).
- Recording of confidential communication without consent.
- Use of illegal “trap and trace” and pen register devices.



Example:

February 21, 2024

Notice of Dispute and Demand
Protected Communication

Re: [REDACTED]

Please be advised that our client below has claims against your company for violation of California privacy law. This letter is a notice of dispute and demand sent pursuant to the pre-arbitration notice of disputes section of your terms and conditions. A synopsis of our client's claims, detailed information on those claims, the applicable law, a demand, the basis of the demand, as well as further settlement discussion points are below.

Claimant's Information

[REDACTED]

Governing Law

Under the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code § 630 et seq ("CIPA"), a person whose communications are illegally tapped, read, or contents are learned is entitled to the following damages:

- \$5,000 per violation, pursuant to Cal. Pen. Code § 637.2.

Courts have ruled that Cal. Penal Code § 631(a) of CIPA is not limited to phone lines, but also applies to "new technologies" such as computers, the internet, and email. See *Matera v. Google, Inc.*, 2016 WL 8200619 at *21 (N.D. Cal. 2016) (CIPA applies to "new technologies" and must be construed broadly to effectuate its remedial purpose of protecting privacy); *Bradley v. Google, Inc.*, 2006 WL 3798134 at *5-6 (N.D. Cal. 2006) (CIPA governs "electronic communications").

Under California common law, claims for intrusion upon seclusion and invasion of privacy involve a similar test, so courts consider the claims together and ask whether: (1) there exists a reasonable expectation of privacy, and (2) the intrusion was highly offensive. *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (2020).

Basis for Demand

[REDACTED] ("Respondent") utilizes tracking software, including a Meta Pixel, that allows Respondent to embed a JavaScript in the HTML code of Respondent's website that intercepts, tracks, stores, and analyzes Claimant's interactions with Respondent's website. By embedding the Meta Pixel within its website, Respondent aided Meta dba Facebook to intercept, store, and analyze Claimant's electronic communications for the purposes of data mining and targeted advertisement.

We downloaded the HTTP Archive Format ("HAR") file from Respondent's website which exposes the vast extent of wiretapping and data mining in which Respondent and its co-conspirator Meta engage. In addition to Meta, Respondent aids other companies in tapping and learning the contents of Claimant's electronic communications with Respondent's website.

Claimant realized this was occurring after finding a detailed list of interactions with Respondent's website in Claimant's personal Facebook account ("off-Facebook activity"). The interactions included Respondent's tracking analysis of Claimant's interactions, each labeled as an "Activity." The information found in Claimant's off-Facebook activity includes (1) Claimant's personalized ID number, (2) the date and time of the activity and (3) the event, or the activity itself (i.e. "Page View" or "Content"). The off-Facebook activity constitutes the tip of the iceberg of the information the Meta Pixel collects. The information in Claimant's Facebook account confirms Respondent embedded a Meta Pixel on Respondent's website which allowed Respondent and Meta to intercept, store, and analyze Claimant's communications for their commercial benefit. The images below depict two data sets which reveal just a snippet of the data obtained by Respondent and Meta by using Meta Pixel on Respondent's website.

Respondent utilizes the Meta Pixel to surreptitiously and covertly gather Claimant's electronic communications and data, which includes, but is not limited to: 1) a full-string, detailed URL for each page on Respondent's website that Claimant views and 2) the website folders and sub-folders on Respondent's web-server, which provides vast quantities of Claimant's data to Facebook. The Meta Pixel script embedded on Respondent's website allows both Respondent and Meta to surreptitiously tap and learn the contents of Claimant's electronic communications. This is the exact factual scenario of which Courts have been concerned; the surreptitious tapping and collection of user data for the purposes of future data mining and benefit.

The information Respondent aided Meta to intercept includes much more than Claimant's IP address and gives rise to serious invasions of privacy and inclusion upon seclusion claims. Respondent's invasion of Claimant's privacy occurred, as the Meta Pixel confirms, within milliseconds – a time where Claimant could not possibly read Respondent's Terms of Use and Privacy Policy, let alone agree to them.

Any alleged consent occurred well after the tapping began. The pixel spyware became active instantaneously upon visiting Respondent's site. Even if Claimant later consented to its use, it would have occurred well after the fact. Such was the case in *Javier v. Assurance IQ, LLC* where

the Ninth Circuit rejected retroactive consent for tapping website users. *Javier v. Assurance IQ, LLC*, No. 21-16351 (9th Cir. May. 31, 2022).

Such an intrusion is highly offensive even to the most reasonable consumer considering that Respondent willingly chose to embed the script on Respondent's website thereby aiding Meta to tap and collect Claimant's communications in a matter of milliseconds. This is not a case where Respondent can claim that the information collected was just for its own private consumption and therefore can avail itself to any "party exception" which could apply. The Ninth Circuit, along with the First and Seventh Circuits have held that the simultaneous, unknown duplication and communication of "GET requests" like those at issue here do not exempt a defendant from liability under the "party exception." Additionally, the key distinction in this case, separate and apart from other claims that Respondent may face, is that Claimant's data was collected instantaneously by both Respondent and Meta for the sole purpose of having the data aggregated, and then independently used and sold.

The images below depict two data sets which reveal just a fragment of Respondent's and Meta's data collection through use of the Meta Pixel which occurs instantaneously when a consumer visits Respondent's website.



(Image confirms Respondent includes Meta Pixel(s) on Respondent's website)

By way of further explanation, what typically occurs when Claimant visits Respondent's website is that Claimant's internet browser sends a GET request to Respondent's website server, which

causes the website to send the information requested by Claimant to Claimant. This communication usually only occurs between the user's web browser and the website being viewed. But on Respondent's website, Respondent placed JavaScript code that allowed Respondent and Meta to track visitor activity by directing the user's browser to copy the referrer header from the GET request and send a separate, but identical, GET request and the associated referrer header to Meta's server. This is the conduct Claimant alleges is unlawful.

The screenshot below provides a screenshot of the HAR file downloaded from Respondent's website and exposes the true extent of the data interception, collection, and dissemination in which Respondent engages. The screenshot is not of Claimant's interactions with Respondent's website; however, Claimant alleges the same data collection and dissemination occurred on the day(s) Claimant interacted with the website.



In this sample, Respondent's website received 90 GET requests from the browser with a total of 4.3 megabits of information collected and disseminated within seconds. Of the 90 GET requests, countless went to separate third parties which included, but were not limited to: Facebook, Google, Car Gurus, and Fox Dealer.

Settlement Demand

Claimant's Facebook data shows that Respondent aided and conspired with Meta to tap and learn the contents of Claimant's sensitive and private electronic communications on at least seven separate occasions within the last year. Claimant will testify to that at the arbitration hearing and the back-end data, confirmed by our expert, will support Claimant's testimony. Each such occasion constitutes a separate violation of Cal. Pen. Code § 631(a) with each violation allowing for \$5,000 in statutory damages.

Respondent's seven interceptions results in a total of \$35,000 in statutory damages under CIPA. Furthermore, GET requests sent to the above-identified third parties results in a total of \$25,000 statutory damages under CIPA. Based on this information, the total amount in statutory damages amounts to \$60,000. This is Claimant's opening settlement demand.

Online Technologies Subject to These Claims

- Online Chat Modules
- Session Replay Tools
- Third-Party Tracking & Analytics
Cookies
- Geotargeting Tools



NY AG Guidance - Consumers

- On July 30, 2024, the Attorney General James' office issued a comprehensive guide on cookie consent banners
- The AG guidance also contains a business guide - "[Business Guide to Website Privacy Controls](#)"
- lays out specific "dos and don'ts" and "mistakes to avoid"
- Based on an AG investigation of the issue
- Reflects policy preference for opting out of cookie tracking
- Overall hostility to Retargeted advertising



The screenshot shows the top portion of the New York State Attorney General's website. At the top, there is a dark blue header with the text "Office of the New York State Attorney General" and a "Translate" button. Below this is the main navigation area, featuring the New York State Attorney General's seal on the left, the name "Letitia James" in a large, bold, blue font, and the title "New York State Attorney General" below it. To the right of the name is a search bar with the placeholder text "Search ag.ny.gov" and a dropdown menu labeled "How can we help you?" with the option "I Want To...". Below the navigation is a horizontal menu with links for "About", "Resources", "Libraries & Documents", "News & Media", and "Contact". The main content area features a light blue background with the headline "Attorney General James Launches Website Privacy Guides for New York Consumers and Businesses" in a bold, dark blue font. Below the headline is a sub-headline: "AG James' Consumer Guide will Help New Yorkers Better Understand How to Safeguard Against Unwanted Tracking Online". The date "July 30, 2024" is displayed in a small, dark blue font. At the bottom, there is a short paragraph of text: "NEW YORK – New York Attorney General Letitia James today announced the launch of two privacy guides on the Office of the Attorney General (OAG) website: a [Business Guide to Website Privacy Controls](#) and a [Consumer Guide to Tracking on the Web](#). The Business Guide will help businesses better protect visitors to their websites by identifying common mistakes businesses make when deploying tracking technologies."

OEM Website Issues

Ongoing dealer concerns about OEM ads on dealer sites

- Raises numerous compliance concerns
- Now - at least one OEM has reportedly begun “requiring” use of OEM site

Other ongoing challenges in the marketplace

- Pressure from marketing companies and others
- To mischaracterize cookies/change/hide
- To work with those who may cut corners





Consent Banners:

What Are They and What Are the Potential Tradeoffs?

- The fundamental issue is what consumer consent will a dealer require before deploying analytics & retargeting cookies on a dealer website.
- Dealers must weigh the business vs legal risks. They could lose up to 40% of visibility into website traffic through tools like Google Analytics from high risk jurisdictions.
- Banners do not “eliminate” analytics or retargeting cookies. They simply ask the consumer for consent - and trends indicate that over **60% of customers accept all cookies**.

COMPLYAUT ✓

Solutions to These Various Issues




Cookie Consent Banner and Comprehensive Privacy Policy

- **Cookie Banners** - A compliant cookie consent banner prevents marketing cookies and tracking pixels from loading until a consumer consents to it by clicking "accept".
- **Privacy Policy** - These should disclose website tools that collect and share information, detailing exactly what categories of information are collected and who they are shared with.
- **Disclosure in chat module** - Work with chat module providers to include a conspicuous disclosure that notifies consumers that sensitive information sent in the module may be shared with third parties.

Recommended style banner

Your Privacy & Cookies

This site deploys cookies and similar tracking technologies, including **essential cookies** for necessary website features, accessibility, and cookie preferences (which may interact directly with, or be shared with, third-party service providers), **functional cookies** for error reporting and to remember settings and delivery optional functionality (including live-chat and other tools, enabling data collection and sharing with third parties), and **marketing cookies** for targeted advertising and analytics. You can reject **marketing cookies** by pressing 'Deny marketing cookies', but we still use essential and functional cookies. By pressing 'Allow All Cookies', you consent to the use of all cookies and the sharing of information they collect with third parties. By continuing to use this site, you agree to our [Privacy Policy](#), which includes an [Arbitration Provision](#), and details the categories of personal information we collect, the purposes for which it is used, and how to exercise your California privacy rights. To stop the sale or sharing of your personal information offline or limit the use of your sensitive personal information, click the pill icon or Your California Privacy Choices link at any time.

 [Your California Privacy Choices](#) [Customize cookie settings](#) [Deny marketing cookies](#) [Allow all cookies](#)

- Auto blocks all marketing cookies until user accepts banner (targeting and analytics)
- Provides notice of sharing with third parties
- Has translation options upon deployment
- User consents to hyperlinked Privacy Policy and receives notice of arbitration provision
- Allows user ability to customize settings
- [New Geofencing](#) - Have different banners for different states

Beware of Dark Patterns

- Not all cookie banners are created equal; both state Attorneys General and the FTC have warned against the use of “dark patterns” in cookie consent banners (CA has outright banned certain dark patterns)
- Dark Patterns are considered a UDAP violation and will not satisfy “express and informed consent”

The image displays four examples of cookie consent banners, illustrating various dark patterns:

- Example 1 (Top Left):** A white banner with a close button (X) in the top right. The text reads: "This website uses cookies and other tracking technologies to enhance user experience and to analyze performance and traffic on our website. We also share information about your use of our site with our social media, advertising and analytics partners. If we have detected an opt-out preference signal then it will be honored. Further information is available in our [Privacy policy](#)". At the bottom, there are two buttons: "Manage cookies" and "Accept all".
- Example 2 (Middle Left):** A white banner titled "Cookie Consent". The text reads: "We use our own and third party cookies to show you more relevant content based on your browsing and navigation history. Please accept all cookies or manage your settings below (see our [cookie policy](#)).". At the bottom, there are two buttons: "Cookie Settings" and "Accept All".
- Example 3 (Bottom Left):** A blue banner titled "This site uses cookies" with a close button (X) in the top right. The text reads: "By proceeding, your agree to our [Privacy Policy](#), including the use of cookies and other tracking tools.". At the bottom, there is a single "Accept" button.
- Example 4 (Top Right):** A yellow banner titled "Welcome to the dealership website". The text reads: "We want to give you the very best service during your car buying experience. 'Accept all Cookies' and you agree to the storing of cookies on your device to improve navigation, site usage, and marketing.". At the bottom, there are two buttons: "Cookie Settings" and "Accept all Cookies".
- Example 5 (Bottom Right):** A white banner with the text: "This website uses cookies, including cookies from third parties, for operational purposes, statistical analysis, personalization, to offer you targeted content that fits your interests, and to measure advertising campaigns. You can accept cookies or modify your choices.". Below the text is a link "Customize cookie consent ->". At the bottom, there are two buttons: "Necessary Only" and "Accept All".

Contractual Relationships

- Beware of representations and warranties in OEM, finance company, and/or advertising partner agreements stating that you (the dealer) have obtained consent from consumers for data collection and sharing with third parties (including sharing with the OEM).
- Consider indemnification in favor of dealer to balance risks
Will need to be negotiated
- Consider enabling Google restricted data processing to have Google act in the context of a “service provider” for compliance within state privacy laws.



FTC CARS Rule

The Basics



Background on the Rule

- Three years in the making. FTC claims it received more than 100,000 complaints regarding motor vehicle sales in each of the past 4 years.
- The most comprehensive and significant set of federal regulations ever introduced in the automotive dealership industry.
- Published regulations are 370+ pages. The core substance of the regulations are primarily found within the FTC's interpretive commentary.
- Effective July 30, 2024.



CARS Rule Fundamentals

- Prohibited Advertising Practices: Enforces a strict set of rules against certain advertising methods.
- "Offering Price" Rules: Requires a clearly displayed advertised price for all vehicles and finance specials.
- Salesperson Communication Rules: Sets guidelines for initial salesperson interactions, including requirement to disclose offering price in first communication.
- Add-on Product Regulations: Bans the sale of what FTC considers non-beneficial products/services, requires optional product disclosures, and mandates inclusion of preloaded "mandatory" add-ons in advertised price.
- New "Payment & Add-on Disclosure" Form? Introduces new requirements to ensure customer consent for add-ons and other dealer chargers, stricter than similar state laws (e.g., California's pre-contract disclosure).
- Monthly Payment Trigger Term Rules: Requires new disclosures whenever a monthly payment is mentioned.
- Record Retention Rules: Imposes comprehensive 24-month record retention requirements.



FTC Delays CARS Rule Effective Date

Federal Trade Commission (FTC) announced that it will delay enforcement of the CARS Rule (Rule) while it faces judicial review. The decision follows the initiation of a legal challenge by the National Automobile Dealers Association (NADA) and the Texas Automobile Dealers Association (TADA), who filed a Petition for Review with the United States Court of Appeals for the Fifth Circuit on January 5, 2024.

Expected decision late Fall 2024

NADA and ComplyAuto join forces

NADA selected ComplyAuto to co-author a manual providing guidance on the FTC CARS Rule in its “Driven Management Guide” series.

COMPLYAUTO ✓

Will the CARS Rule go away?

- Exercise enforcement action under the FTC Act - Unfair, Deceptive Acts and Practices (UDAP)
- The Junk Fee (Hotel Rule) could be carried over to dealers if the FTC CARS Rule doesn't go into full effect
- FTC Commissioner terms are seven years (some terms expire 2028)
- Representation/FTC Commissioner appointments are supposed to come from both political parties



Recent Enforcement Actions

PA - 11/16/2023 - State AG - Penalty not specified

[Fraud, failure to provide paperwork](#)

PA - 8/10/2023 - State AG - penalty not specified

[Fraud, failure to provide paperwork](#)

PA - 6/9/2023 - State AG - Penalty not specified

[Fraud, failure to provide paperwork](#)

OH - 2/29/2024 - State AG - Not specified

[Deceptive sales & advertising practices, titling issues](#)

RI - 8/15/2024 - State AG - penalty \$1 million

[Deceptive sales and advertising practices, add-ons](#)

MD - 8/1/2024 - State AG - \$10,000 per car

[Deceptive sales & advertising practices](#)

KS - 8/10/2024 - State AG - penalty \$159,000

[Deceptive sales & advertising practices, titling issues](#)

MN - 4/23/2024 - State AG - penalty Not specified

[Deceptive sales & advertising practices](#)

IN - 7/17/2024 - State AG - penalty \$500,000

[Deceptive sales & advertising practices](#)

NY - 3/28/2024 - State AG - penalty \$1.9 million

[Deceptive sales & advertising practices](#)

AZ - 3/18/2024 - State AG - penalty \$60,000

[Deceptive sales & advertising practices](#)

AZ - 8/15/2024 - FTC & State AG - penalty \$2.6 million

[Deceptive sales & advertising practices, discriminatory practices, junk fees](#)

National Used Car Dealer - 7/16/2024 - FTC = \$1 million+

[Deceptive sales and advertising practices](#)

CT - 1/4/2024- FTC & State AG - rescission and damages sought

[Deceptive sales and advertising practices](#)

CT - 5/28/2024 - State AG - penalty not specified

[Deceptive sales and advertising practices, add-ons](#)

WI - 11/6/2023 - FTC & State AG - \$1.1 million

[Add-ons, discriminatory practices](#)

MD - 5/16/2023 - FTC - penalty \$3.3 million

[Add-ons, discriminatory practices](#)

IL - 4/1/2022 - FTC - \$10 million

[Add-ons, discriminatory practices](#)

RI - 7/26/23 - State AG - penalty \$557,815

[Deceptive sales and advertising practices, add-ons](#)

RI - 3/7/2023 - State AG - penalty \$30,000

[Deceptive sales and advertising practices, add-ons](#)

TX - 8/16/2024 - FTC - Admin Complaint

[Deceptive sales and advertising practices, add-ons](#)

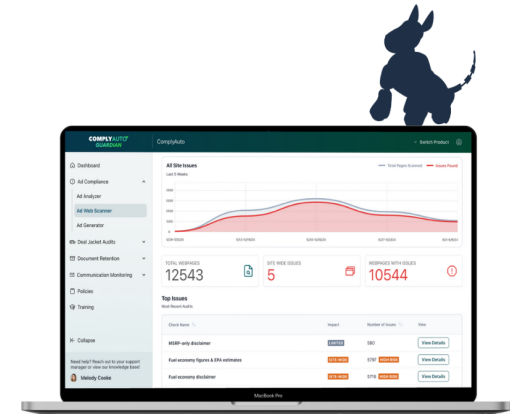
AK - 8/9/2023 - State AG - \$25k per violation

[Deceptive sales and advertising practices](#)

COMPLYAUTO GUARDIAN

Adopt the First AI of Its Kind

Guardian eliminates dealers' biggest compliance exposures with a full set of sales and F&I compliance features.



Deal Jacket
Auditing



Policy &
Forms
Library



FTC
Compliance



Online F&I
Training



AI
Monitoring



Record &
Vendor
Management

Questions?

COMPLYAUTO



Nick.Moyes@ComplyAuto.com

10,000+ active
dealers across all
50 states

40+ state dealer
association
endorsements



COMPLYAUTO
PRIVACY