

VENDOR SECURITY TRANSPARENCY STUDY

Assessed on Faith

What a dealer can actually verify about the software suppliers they are legally required to assess

147 brands · 126 independent companies · security and trust pages only

Prepared by **Andrew Tubbs**

CISSP, CISM, C|CISO — formerly Director, Information Security, Cox Automotive

September 2026

Published by **Level Four LLC** · l4is.ai

Version 1.0 · DOI 10.5281/zenodo.23600828



PUBLISHED EDITION. AGGREGATE FIGURES ONLY. NO VENDOR IS NAMED ALONGSIDE ITS OWN RESULTS; A COMPANY APPEARS BY NAME ONLY WHERE THAT COMPANY PUBLISHED SOMETHING ITSELF, AND THEN AS CREDIT RATHER THAN AS A SCORE.

Contents

Executive summary.....	3
Why dealers started checking.....	5
Findings.....	7
What it means.....	10
Which framework to build to first.....	11
Methodology.....	12
What enforcement actually looks like today.....	13
Corporate ownership and the unit of analysis.....	15

Executive Summary

Every dealership that finances or leases vehicles is a financial institution under the FTC Safeguards Rule, 16 C.F.R. § 314.4, and § 314.4(f) requires each of them to select service providers capable of maintaining appropriate safeguards, bind those providers by contract, and reassess them periodically. The Rule never specifies what that assessment must contain — only that it must happen. In practice it begins the same way every time: someone at the dealership opens the supplier’s website and looks for evidence.

This study measured what that person finds. One hundred and forty-seven vendor brands, operated by one hundred and twenty-six independent companies, were assessed against two layers of entirely public signal — email authentication published in DNS, and security documentation published on the web. One hundred and forty-five brands, operated by one hundred and twenty-four companies, could be scored on the web layer; two could not be reached at all and are excluded rather than counted as publishing nothing.

The central finding is not that these companies are insecure. It is that they are opaque — and that the opacity is very nearly universal.

Two consequences follow, and neither is an abstraction. A dealer obliged to assess a supplier has, in most cases measured here, nothing to assess — so the assessment becomes a questionnaire, and the questionnaire becomes a delay inside the supplier’s own sales cycle. And a supplier that has not published an email policy leaves its customers’ finance offices reachable by anyone willing to forge its domain: a loss the dealership carries and the supplier’s name is attached to.

Principal findings

1	Twenty-three brands out of the one hundred and forty-five whose sites could be read publish a discoverable way to report a security vulnerability — but nine of those are Cox Automotive brands sharing a single group security.txt file.
2	Sixty-two percent of companies publish none of the four signals a reviewer needs — no security or trust page, no disclosure route, no sub-processor list, no breach notification terms.
3	Eighteen brands publish a sub-processor list. Four publish breach notification terms. These are the two signals a vendor questionnaire depends on most directly, and they are the two least published.
4	Roughly three brands in ten publish either no email authentication policy or one set to take no action, leaving their domain forgeable.
5	Seventy-four percent of those brands already have both mechanisms DMARC requires. They stopped one DNS record short of the policy that would make any of it count.
6	The gap does not track company size smoothly. Large and mid-size companies are indistinguishable from each other; small companies are the break.

Why this lands on the dealer

Under the Safeguards Rule, a compromise of dealer customer information is reported as the dealer’s breach. The Commission’s public database names the dealership, not the software company whose product was the point of failure. The dealer therefore carries a regulatory exposure created by a supplier whose security posture they are obliged to assess and, in most cases measured here, cannot.

The practical consequence is an inversion. The suppliers easiest for a dealer to assess are the large ones that least need assessing. Those holding the same categories of regulated customer data with a fraction of the security apparatus publish nothing at all.

What this study does not claim

It measures disclosure, not security. A company that publishes nothing may be well run; one with a polished trust page may not be. Nor does it measure compliance: the Safeguards Rule binds the dealer, not the supplier, and nothing assessed here is something the Rule obliges a vendor to publish. The findings establish something narrower and, for a dealer, more immediately useful — whether there is anything to look at when they are obliged to look.

Why Dealers Started Checking

Four events in roughly two years changed how a dealership looks at the software it buys. They differ in kind — an outage, a breach, a regulator and a market for stolen documents — and none of them is a Safeguards Rule matter. Together they are why a supplier questionnaire that used to be a formality is now a gate.

June 2024 — availability. Ransomware against CDK Global took roughly fifteen thousand dealerships offline for about two weeks. Anderson Economic Group estimated direct dealer losses at \$944 million in the first three weeks alone. Every dealer principal and group chief financial officer in the country lived through it, and the lesson was that a supplier's outage is the dealership's outage: the store cannot sell, deliver or pay people, and nothing in its own security program prevents that.¹

October 2025 — confidentiality. 700Credit, a credit and compliance provider whose own materials describe more than twenty thousand dealer customers, discovered on 25 October that an intruder had been in its environment since the preceding May. The exposure covered more than 5.8 million people and included names, addresses, dates of birth and Social Security numbers. A proposed settlement has been preliminarily approved, with a final approval hearing set for October 2026. The company is a brand of Open Dealer Exchange, LLC, which its own site describes as a joint venture founded by CDK Global and Reynolds & Reynolds. The lesson is sharper than the first: the vendor was breached, the victims were dealership customers, and the dealership is the party holding the relationship with them.²

Through 2026 — a regulator that acts. The Federal Trade Commission has been visibly active against automobile dealers, though not on data security. It issued warning letters to ninety-seven dealership groups in March 2026 over deceptive pricing; it settled with Lindsay Automotive Group and the Maryland Attorney General in April, with more than seventy-five million dollars in consumer refunds and a \$3.1 million civil penalty; and in August it reached a four-million-dollar settlement with Manchester City Nissan alongside the Connecticut Attorney General. All of that is pricing and conduct under Section 5 of the FTC Act rather than § 314.4, and this report says so plainly in its enforcement section. What it establishes is narrower and still material: the Commission will bring actions against dealers, and when it does the dealer is the named party. Under § 314.4(j) the same is true of a security failure — a breach touching five hundred or more consumers' unencrypted information is reported to the Commission in the dealer's name, in a public database, whether or not it originated at the dealership.³

August and September 2026 — the document itself. A subscription service advertised on a Russian-language cybercrime forum was found to be selling access to more than 153 million United States and Canadian driver's license images, together with identification cards, travel documents and medical cards. The images are alleged to have come from the pipeline of an identity-verification vendor whose own marketing offers license scanning to car dealerships for test drives and F&I. The FBI's New Orleans field office opened an inquiry after the service was publicly reported on 31 August 2026. The allegations are unproven; this study holds the company named in that reporting out of its sample entirely pending the inquiry, and does not name it here. The point does not depend on the outcome. A driver's license is the document a dealership copies more often than any other, it is increasingly captured by a vendor rather than by the store, and the store's own controls have no bearing on what happens to it afterwards.⁴

What changed across these four is not dealer opinion of any particular supplier. It is that vendor due diligence stopped being a formality. A security questionnaire arriving late in a sales cycle is now routine, and the people sending them are themselves being audited on whether they sent them.

¹ Anderson Economic Group, estimate of dealer losses from the CDK Global outage, June 2024.

² 700Credit, consumer breach notification, October 2025, and contemporaneous reporting; Open Dealer Exchange, LLC, corporate description, accessed September 2026.

³ Federal Trade Commission, "FTC Warns 97 Auto Dealership Groups About Deceptive Pricing," press release, March 2026; Federal Trade Commission and Maryland Attorney General, Lindsay Automotive Group settlement, April 2026; Federal Trade Commission and Connecticut Attorney General, Manchester City Nissan settlement, August 2026.

⁴ Contemporaneous reporting of the identity-verification matter, August–September 2026; Federal Bureau of Investigation, confirmation of an open inquiry, September 2026. Allegations are unproven and the company is held out of this study's sample.

That is the environment this study describes. It is not a story about negligence; it is a story about an industry being asked, for the first time and all at once, to show its work.

Findings

What a dealer can discover

Each brand's public site was requested at the conventional locations a reviewer or automated tool would try, together with the homepage, its trust subdomains, /.well-known/security.txt, and every link on the homepage whose text or address mentions security, trust, compliance, disclosure or a named standard. The table below reports the share of the one hundred and forty-five brands whose sites could be read where each signal was found.

SIGNAL	FOUND	OF	SHARE
Security or trust page	44	145	30.3%
SOC 2 mentioned publicly	44	145	30.3%
Vulnerability disclosure route	23	145	15.9%
Penetration testing mentioned	20	145	13.8%
ISO 27001 mentioned	19	145	13.1%
Sub-processor list	18	145	12.4%
MFA or single sign-on documented	12	145	8.3%
Breach notification terms	4	145	2.8%

One might expect product security features to be advertised while organizational evidence stays quiet. The data does not support even that much. The three signals a dealer's vendor questionnaire most directly depends upon — a disclosure route, breach notification terms, and a sub-processor list — appear at 15.9, 2.8 and 12.4 percent by brand. MFA, a feature that belongs on a pricing page, appears at 8.3 percent, lower than two of the three. Nothing is being advertised in place of the evidence. Almost nothing is published at all.

Counted per company, sixty-two percent publish none of the four review signals — a security or trust page, a vulnerability disclosure route, a sub-processor list, and breach notification terms. Fifteen companies publish a vulnerability disclosure route; more than a third of the twenty-three brands that do are Cox Automotive brands covered by one group security.txt.

Where the gap concentrates

Publishing concentrates at a single break in company size, and not by product category at all.

SIZE BAND	COMPANIES	SECURITY PAGE	DISCLOSURE ROUTE
Large	18	8 (44.4%)	4 (22.2%)
Mid-size	42	19 (45.2%)	6 (14.3%)
Small	50	13 (26.0%)	5 (10.0%)
Unknown size	14	2 (14.3%)	0 (0.0%)
All companies	124	42 (33.9%)	15 (12.1%)

Thirteen of the fifty small companies publish a security page, against eight of eighteen large and nineteen of forty-two mid. Large and mid are indistinguishable from one another — an odds ratio of 0.97 at $p=1.000$ — while small companies sit meaningfully behind both, at an odds ratio of 2.33 and $p=0.048$. The three-way gradient across all bands is not significant (chi-square 4.26, $p=0.119$). It is a break rather than a slope, and it falls between small companies and everyone else. The break is specific to the security page: on SOC 2 the bands are no longer distinguishable ($p=0.84$), because certification claims in this market are frequently carried by a footer badge rather than by a page, and small companies publish badges as readily as large ones. Fourteen companies have no reliable size band; they are shown separately and held out of the tests rather than guessed. On vulnerability disclosure the rate is low at every size: fifteen companies in the whole study publish one.

Email authentication

The costliest fraud pattern in automotive retail does not involve breaking into anything. A message arrives at a dealership's finance office from a supplier the store already works with — a change of bank details on an invoice, an attachment, a request that looks routine because it looks familiar. Nothing at the supplier is compromised. The message is forged, and it is delivered because nothing published by the supplier told the receiving mail server to refuse it.

Only the domain owner can stop it, and the instrument is a single published instruction. A DMARC policy tells every receiving mail server that checks — and the large providers do check — how to treat mail that forges the domain: $p=reject$ refuses it, $p=quarantine$ diverts it to spam, and $p=none$ takes no action at all. It costs nothing, requires no software, and a customer cannot publish it on the supplier's behalf however diligent that customer is. It is also verifiable by anyone in seconds, which makes it the one control in this study a dealer can confirm without asking.

That asymmetry is why this belongs in a commercial discussion rather than a technical appendix. The dealership bears the loss, the supplier's name is on the message, and the only party able to prevent it is the one not paying for it. Read the other way, a supplier already at enforcement holds something unusual in this market: a security claim a prospect can verify in seconds, and that most of its competitors cannot make.

SIZE BAND	BRANDS	REJECT	QUARANTINE	UNPROTECTED
Large	28	18 (64.3%)	6	4 (14.3%)
Mid-size	50	20 (40.0%)	19	11 (22.0%)
Small	53	12 (22.6%)	20	21 (39.6%)
Unknown size	14	2 (14.3%)	5	7 (50.0%)
All brands	145	52 (35.9%)	50	43 (29.7%)
Per company	124	37 (29.8%)	47	40 (32.3%)

The machinery is built; the policy is not switched on

Querying twenty-five well-known DKIM selectors detected a published key for one hundred and thirty-five of the hundred and forty-seven brands. Detection is deliberately one-directional and reported that way: a hit proves presence, a miss is recorded as unknown, never as absence, because selectors cannot be enumerated from DNS.

What this adds is not another score. It answers the question the rest of the email findings leave hanging — whether these companies are careless or merely unfinished.

POSITION	BRANDS	WHAT REMAINS
DMARC already at quarantine or reject	102	Enforcement in place. DKIM confirmed present for 97.
Mechanisms ready, policy missing	32	SPF and DKIM both working at p=none. One record from enforcement.
Mechanisms unconfirmed	11	No DKIM key found at a well-known selector — unknown, never absence — or SPF not established.

Seventy-four percent of the unprotected brands already have both mechanisms DMARC requires — the remainder are unconfirmed rather than known to lack them. They authenticated their mail, aligned their senders, and stopped one DNS record short of the policy that would make any of it count.

What It Means

For dealers

The DNS checks in this study take seconds per supplier and require nothing from the supplier. Under § 314.4(f) a dealer is already obligated to assess service providers, and this is the least expensive evidence available toward that obligation.

The more useful question at contract renewal is not whether a supplier is secure, a question no supplier answers no to, but where their security documentation is published and how a vulnerability would be reported to them. Both have verifiable answers, and a supplier unable to give either has told you something material.

One procedural note: a portfolio of brands under a single parent should be assessed once at the parent level and then tracked per domain. The corporate security program is shared; the DNS records are not.

For suppliers

The commercial case is stronger than the security case. A security questionnaire is a procurement delay arriving late in the sales cycle; published disclosure converts it from work done once per prospect into work done once.

Companies selling questionnaire-automation software report that most organizations take more than two weeks to complete a manual vendor assessment, that a majority have lost deals to the delay, and that account executives spend around seven hours a month on questionnaire work. Those figures should be treated as advocacy given their source, but they point at a mechanism nobody in enterprise sales disputes.

There is also a risk the disclosure finding understates. A researcher who cannot reach a supplier does not stop looking; they publish, or they tell one of that supplier's customers. For the hundred and nine companies here with no published security contact, the first notice of a vulnerability would arrive from a dealer principal or a journalist rather than from the person who found it.

What closing the gap actually involves

The work divides into four rungs, and the first two cost effectively nothing.

1	Publish what is already true	Days · free	A trust page listing what you already do. Highest return on effort of anything in this report.
2	Turn on the email policy	30–60 days · free	For 74% of the unprotected, SPF and DKIM already work. Move DMARC to quarantine, watch reports, then reject.
3	SOC 2 Type II	3–6 months · \$40–95K	Roughly \$25–45K readiness plus \$15–50K audit. The one buyers name.
4	Build the program underneath	6–18 months · varies	If there is no risk assessment, no incident response plan and no access review, this is the actual work.

A truthful trust page cannot be published for controls that do not exist. Which rung a company is on is what a gap assessment establishes, and it is not always the rung they expect.

Which framework to build to first

There is a sequencing question underneath the four rungs. If a supplier is going to build a security program at all, which framework should it build to first? For a company selling into auto retail the answer is the Safeguards Rule — and not because it is the supplier's law, since it is not. It is that 16 C.F.R. § 314.4 happens to be the smallest coherent control set aligned with what the questionnaires ask — and the control work, though not the management-system work above it, carries forward as the bar rises.

The Rule's eighteen elements are, functionally, a compact control framework. They map cleanly onto the frameworks a buyer will eventually name by title.

Safeguards elements	NIST CSF 2.0	ISO/IEC 27001:2022	What an auditor asks to see
(a) Qualified Individual, (g) evaluate and adjust, (i) board reporting	Govern	Clause 5 leadership; Clause 9 management review	A named owner, a program charter, board minutes
(b) risk assessment, (c)(2) asset inventory	Identify	Clause 6 planning; A.5.9 inventory of assets	A written, periodic risk assessment and an asset register
(c)(1) access control, (c)(3) encryption, (c)(4) secure development, (c)(5) MFA, (c)(6) disposal, (c)(7) change management, (e) training	Protect	A.5.15–5.18, A.6.3, A.7.10, A.7.14, A.8.2–8.5, A.8.10, A.8.24–8.32	Policies, plus evidence that they actually operate
(c)(8) logging and monitoring, (d)(1) control testing, (d)(2) pen test and vulnerability assessment	Detect	A.8.8, A.8.15–8.16; Clause 9.1	Log retention, test reports, remediation records
(h) incident response plan, (j) FTC notification	Respond	A.5.24–5.28	A written plan, exercise records, a notification procedure
(f) select, contract with and reassess service providers	Govern / Identify	A.5.19–5.23 supplier relationships	A vendor inventory, contract clauses, assessment records

What the Rule does not give you

It is a floor, not an equivalence, and nobody should present it as one. ISO 27001 adds an entire management system on top of the control set — a defined scope, a Statement of Applicability, documented objectives, an internal audit program, management review and continual improvement — together with ninety-three Annex A controls, and it ends in a certificate issued by an accredited body. SOC 2 Type II adds an independent auditor testing operating effectiveness across a period, which is a materially different exercise from having the control. NIST CSF is not certifiable at all; it is an outcome and maturity language, which is exactly what makes it useful for talking to a board.

The difference is evidentiary discipline rather than control coverage. Safeguards asks a company to do the thing. ISO and SOC 2 ask it to prove, to a third party, that it kept doing the thing.

A sequence that wastes nothing

- 1. Build to § 314.4.** The smallest coherent control set, and the natural yardstick for the assessment a supplier's customers are legally obliged to perform.
- 2. Publish it.** The trust page converts the control work into a sales asset, and whatever cannot yet be written down is the roadmap.
- 3. SOC 2 Type II.** The attestation buyers name in questionnaires. Every artifact from step one is evidence here.
- 4. ISO 27001, when it is asked for.** International buyers, OEM procurement, or a transaction process are what trigger it — not ambition.

5. Keep NIST CSF as the internal lens throughout. It is free, it maps to all of the above, and it is the only one of them that gives a board a maturity-style conversation — via Implementation Tiers, which NIST notes are not formal maturity levels — rather than a pass or fail.

Each rung is built out of the rung below it, which is what makes starting at the floor the capital-efficient choice rather than the modest one. The order matters more than the pace.

Methodology

Two categories of lookup were performed, both against entirely public information. DNS TXT queries retrieved each domain's DMARC and SPF records, and queried twenty-five well-known selectors for a published DKIM key — the same queries every receiving mail server on the internet performs continuously. Ordinary HTTPS requests retrieved each brand's homepage and a short list of conventional security-page paths, exactly as a web browser would load them.⁵

SCOPE OF ACCESS. Nothing was scanned, probed, or tested. No ports, no vulnerability testing, no authentication attempts, no credentials, and no request that a normal visitor or mail server would not make. This applied to every vendor without exception.

What the Safeguards Rule requires

The Rule places its duties on the financial institution — the dealer. It imposes no direct obligation on a software supplier at all; a supplier is reached only indirectly, through § 314.4(f). Critically, the Rule does not specify what that assessment should consist of, only that it must happen and be risk-based. The market filled that gap with trust pages, SOC 2 reports and standard questionnaires, and it is those market expectations rather than the regulation from which most of the signals in this study derive.

§	REQUIREMENT	§	REQUIREMENT
(a)	Designate a Qualified Individual	(c)(7)	Change management procedures
(b)	Written, periodic risk assessment	(c)(8)	Monitoring and logging of user activity
(c)(1)	Access controls; least privilege	(d)(1)	Regularly test key controls
(c)(2)	Inventory data, systems and devices	(d)(2)	Continuous monitoring — or annual pen test + 6-monthly vulnerability assessment
(c)(3)	Encrypt customer data in transit and at rest	(e)	Security training and qualified personnel
(c)(4)	Secure development practices	(f)	Select, contract with and reassess providers
(c)(5)	Multi-factor authentication	(g)	Evaluate and adjust the program
(c)(6)	Secure disposal within two years	(h)	Written incident response plan
		(i)	Qualified Individual reports to the board
		(j)	Notify FTC ASAP, no later than 30 days (500+ consumers, unencrypted)

⁵ RFC 7489 (DMARC) and RFC 9116 (security.txt) govern the records queried. DNS and web data were collected 5 September 2026.

What could not be measured

Of those eighteen discrete elements, none can be fully verified from outside the organization and only three are even partially inferable.

PARTIALLY INFERABLE	WHAT CAN BE SEEN	WHAT CANNOT
§ 314.4(c)(3) Encryption	TLS on the public site	Encryption at rest — the part that matters
§ 314.4(c)(5) MFA	Whether the product supports it	Whether it is enforced internally
§ 314.4(d)(2) Testing	A stated cadence, if published	Whether tests happen, or what they found

Everything that actually constitutes a security program — the risk assessment, the access controls, the logging, the incident response plan, the board reporting — requires internal access to confirm. This study has none, by design. That cuts both ways: a company scoring badly here may run a disciplined program and simply not talk about it, and a company scoring well may have a well-written page over very little.

What enforcement actually looks like today

A study framed on the Safeguards Rule invites an obvious question, and should answer it plainly. As of September 2026, no Federal Trade Commission enforcement action against an automobile dealer under the Safeguards Rule is publicly identifiable. The Commission's automobile industry docket, its Safeguards Rule legal library, and the dealer-specific Safeguards FAQ it published in August 2025 contain no such matter. That FAQ is written as compliance assistance rather than as a warning.⁶

The Commission is nonetheless active against dealers, on an entirely different footing. In March 2026 it issued warning letters to ninety-seven dealership groups over six deceptive-pricing practices, all under Section 5 of the FTC Act. Asbury Automotive Group is in a pending administrative proceeding over allegations of payment packing and discrimination, which Asbury disputes. Lindsay Automotive Group settled with the Commission and the Maryland Attorney General in April 2026, with more than seventy-five million dollars in consumer refunds and a \$3.1 million civil penalty, and in August 2026 the Commission and the Connecticut Attorney General reached a four-million-dollar settlement with Manchester City Nissan. State attorneys general have produced substantial outcomes of their own — twenty million dollars in Illinois and \$3.2 million in New York among them. None of it concerns data security.⁷

Why this is stated rather than left out

Nobody should tell a dealer or a supplier that the FTC is fining people over this, because it is not. An enforcement claim that cannot be evidenced hands a skeptical reader one sentence with which to dismiss everything else.

The argument does not need enforcement in order to hold. The pressure this study describes comes from two places that are observable today. Under § 314.4(j) a breach involving the unencrypted information of five hundred or more consumers is reported to the Commission, and every such report is accessible in a publicly available database that names the reporting institution — the dealer — rather than the supplier where the incident originated. And since June 2024 dealers have been conducting vendor due diligence as a matter of course rather than as a formality. Neither depends on an enforcement action existing, and the second is what actually determines how quickly a supplier's deals close.⁸

⁶ Federal Trade Commission, Automobile Dealers and the FTC's Safeguards Rule — Frequently Asked Questions, August 2025; Federal Trade Commission automobiles industry docket and Safeguards Rule legal library, accessed September 2026.

⁷ Federal Trade Commission, "FTC Warns 97 Auto Dealership Groups About Deceptive Pricing," press release, March 2026; Lindsay Automotive Group settlement, April 2026; Manchester City Nissan settlement, August 2026.

⁸ 16 C.F.R. § 314.4(j); Federal Trade Commission publication of Safeguards notifications in a public database, requirement effective May 2024.

Whether the current warning letters become enforcement remains to be seen. The Commission's attention is demonstrably on this industry. It is simply not, so far, on this Rule.

Why these nine signals

SIGNAL	IN THE RULE?	BASIS FOR INCLUSION
MFA / SSO supported	Yes — § 314.4(c)(5)	Required of the dealer for anyone accessing any information system. Where the supplier's product holds the data, the dealer cannot comply unless the supplier supports it.
Penetration testing	Yes — § 314.4(d)(2)	Required of the dealer — annual tests, or continuous monitoring. Commonly extended to suppliers holding their data.
Breach notification terms	Indirect	No duty on the supplier, but the dealer's 30-day FTC clock under § 314.4(j) depends on being told.
Sub-processor list	Indirect	No duty on the supplier and no flow-down language in § 314.4(f). Included because capability is hard to judge without it.
Security or trust page	No	Market practice. The practical entry point for the periodic assessment § 314.4(f)(3) requires.
Vulnerability disclosure route	No	Industry norm (ISO/IEC 29147), not regulation.
SOC 2 / ISO 27001	No	Not named anywhere in the Rule. Simply the evidence dealers most often accept.
DMARC / SPF / DKIM	No	Absent from the Rule. The only controls in this set observable with no cooperation from the supplier.

Three constraints drove the selection, in order of precedence: observable without touching the supplier, which was absolute and excludes almost every control the Rule names; binary rather than a matter of judgment; and something a dealer's reviewer would actually look for.

HOW TO STATE THIS, AND HOW NOT TO. Defensible: "most suppliers publish nothing a dealer could use to complete the assessment the Safeguards Rule requires of them." Not defensible: "most suppliers are non-compliant with the Safeguards Rule." The second claim is simply wrong — the Rule does not bind them.

Why SPF is a footnote and DMARC is the finding

Under RFC 7489, DMARC passes if either SPF or DKIM produces a pass that is aligned with the visible From: domain, and DMARC treats the SPF result categorically — an aligned pass, or not. The SPF qualifier therefore makes no difference to a DMARC outcome: a softfail and a hardfail are both simply not a pass. For the hundred and four brands publishing DMARC at quarantine or reject, SPF strength is irrelevant to whether forged mail is stopped.

For the remaining forty-three, SPF is the only line and it is a weak one for a reason easily missed. SPF authenticates the envelope sender, not the From: header the recipient sees. An attacker can pass SPF using a domain they control while displaying the supplier's name and address in the visible From: field. Only DMARC's alignment requirement ties the two together. Thirteen of those forty-three publish a hard fail, which helps against some classes of abuse but does not stop the impersonation pattern that matters here.

THE PRACTICAL CONSEQUENCE. DMARC is the load-bearing control. SPF and DKIM are the mechanisms it evaluates, not alternatives to it. A supplier publishing a hard-fail SPF policy alongside p=none has the parts but not the policy.

Corporate ownership and the unit of analysis

Counting brands rather than companies changes the picture materially. Cox Automotive alone operates nine of the brands assessed; eleven further corporate families account for another twenty-four. Deduplicating to the parent removes twenty-one brands and leaves one hundred and twenty-six independent companies, which is the unit used for every company-level figure in this report.

PARENT COMPANY	BRANDS	CATEGORIES REPRESENTED
Cox Automotive	9	Marketplace, DMS, Inventory, Digital Retail, F&I
CDK Global	3	DMS, Dealer CRM, Digital Retail
Mobility Global	3	Inventory / Data, F&I, Marketing
ACV Auctions	2	Inventory / Data
CallRevu	2	Communications / Call Intelligence
CarGurus	2	Marketplace / Leads
Cars Commerce	2	Marketplace / Leads, Marketing / Web
DealerOn	2	Marketing / Web
Dominion Enterprises	2	DMS / Ops, Dealer CRM
PureCars	2	Dealer CRM, Marketplace / Leads
Solera	2	Dealer CRM, Fixed Ops
Vehlo	2	Fixed Ops

Counted by brand, twenty-three vendors publish a vulnerability disclosure route and the result reads as a property of large companies. Counted by company, nine of those twenty-three are a single Cox Automotive security.txt file served across the group. Fifteen companies in the entire study publish a disclosure route, and a substantial part of the apparent size effect was one conglomerate appearing nine times.

One corporate family illustrates the rule. Two of its three brands publish DMARC at p=reject; the third — a brand the group acquired, whose domain now redirects to the parent's site — publishes no enforcement policy at all. Under a worst-brand rollup, which this report uses because a family is only as forgeable as its weakest domain, that one inherited domain places the whole group in the unprotected column of the per-company table alongside two siblings at enforcement. An acquired brand's domain outlives the brand, and it stays forgeable while it does.

CONFLICT OF INTEREST. The author spent six years as Director of Information Security at Cox Automotive, responsible for Autotrader, Dealer.com, Dealertrack, Kelley Blue Book, vAuto, VinSolutions and Xtime — seven of the nine Cox brands in this sample. He did not work on Cox Automotive Dealer Floor Plan (NextGear Capital) or the Cox Automotive corporate domain, both of which are also in the sample. He departed in March 2025. Cox Automotive publishes a vulnerability disclosure route, one of fifteen companies in this study that does, and its brands are disproportionately represented among the stronger results. No part of this assessment used non-public information, and Cox brands were measured by the identical automated method applied to every other domain. Several of the controls measured favorably at Cox brands were implemented during the author's tenure, and Cox results should be

read as context for the method rather than as independent findings. Separately, the author operates an independent security consultancy serving this market. The consultancy has commercial relationships with companies in this market, which may include companies in the sample. No vendor paid for, commissioned, reviewed or influenced this study, and the dataset was collected before any such engagement was discussed. The reader is entitled to weigh that affiliation, and it is stated here rather than left to be discovered.

Which unit is correct

It depends on the question, so this report gives both. For organizational disclosure the company is the correct unit, because those are corporate policies. For email authentication the brand is defensible, because each domain is independently forgeable.

MEASURE	PER BRAND	PER COMPANY
Vulnerability disclosure route	23 / 145 (15.9%)	15 / 124 (12.1%)
Security or trust page	44 / 145 (30.3%)	42 / 124 (33.9%)
Publishes none of the four	87 / 145 (60.0%)	77 / 124 (62.1%)
DMARC at p=reject	52 / 145 (35.9%)	37 / 124 (29.8%)
DMARC unprotected	43 / 145 (29.7%)	40 / 124 (32.3%)

Deduplication changes the disclosure figure most. The industry looked better on that signal than it is because one corporate family was being counted nine times over.

Sample, reliability and limitations

One hundred and fifty-five vendor brands were assembled from public directories, category listings and the NADA Show exhibitor list, weighted toward companies handling regulated dealer customer data. Eight were removed — two for domains that no longer resolve, three because the domain now serves an unrelated business, two because scoring them double-counted a parent already in the sample, and one because its site is a decommissioned stub that no longer offers the product. That leaves 147 brands, operated by 126 independent companies. Of those brands, 145 could be verified, representing 124 distinct companies; two — Black Book and Upstart Auto Retail — could not be reached at all and are excluded rather than counted as publishing nothing. Every rate in this report, email authentication included, is calculated on those 145 brands and 124 companies.

A failed lookup and an absent record are indistinguishable unless the collection tool is built to separate them, and conflating the two produces false negatives about real companies. The collector returns an explicit failure state, and any vendor whose lookup fails is excluded from the relevant statistic rather than counted against. No DMARC lookup reported here failed. Thirty-two SPF lookups did fail, on domains with large TXT record sets, and are recorded as not verified rather than as absent. Twenty-eight of the thirty-two publish DMARC at enforcement, where SPF strength does not affect the outcome; the other four publish no enforcement policy, so for those SPF is the only line and it is the one this study could not verify.

Each domain was verified to resolve, and confirmed against the company's own site as the domain it actually uses rather than inferred from its name. A hyphenated or marketing variant of a supplier's domain can publish no DMARC record while the domain the company genuinely sends from enforces at p=reject. A single character separates a correct result from a published falsehood about a real business.

What the method undercounts

- Keyword matching misses paraphrase. A supplier describing sub-processors as “third parties we share data with” would not register. The web-layer negatives remain a floor rather than a census; every positive was verified by hand, because automated keyword matching on its own accepts pages that are not security documentation.
- Collection follows every link on a vendor’s own homepage whose text or address mentions security, trust, compliance, disclosure, SOC 2, ISO 27001 or penetration testing, and requests /.well-known/security.txt on every domain per RFC 9116. Path-guessing and a DNS subdomain sweep alone are not sufficient: real, published security pages live at addresses no fixed list would reach, such as /legal-and-trust/, /cyber-and-information-security/ and /soc-2-type-ii. Documentation at an unconventional path with nothing at all linking to it would still be missed — though that is arguably itself a finding, since a dealer’s reviewer would not find it either.
- A trust portal can be hosted on the portal vendor’s own domain rather than on a subdomain of the company’s, in which case no DNS sweep of that company’s domain will ever find it. One was found only by following a homepage link. Where a company’s posture is published by its parent or operator, it is counted for the brand only when a link on the brand’s own site reaches it and that link is labeled for security, or when the artifact is served on the brand’s own domain. Documentation living at an unconventional path with nothing at all linking to it would still be missed — though that is arguably itself the finding, since a dealer’s reviewer would not find it either.
- DKIM detection is one-directional. A hit proves presence; a miss is recorded as unknown, never as absence, because selectors cannot be enumerated from DNS.
- Corporate ownership may be incomplete. Cox Automotive’s nine brands were confirmed directly; the eleven smaller families were identified from public sources and should be independently verified. Three ownership changes observed during collection are reflected in the group table: Cox Automotive has announced an agreement to acquire Fullpath, roadster.com now redirects to cdkglobal.com, and fixedopsdigital.com now redirects to TradePending. Each affected brand is retained as a separate row because its domain remains independently forgeable.
- Size bands are estimates drawn from public sources and have not been confirmed with the companies.

DNS and web data were collected 5 September 2026. DNS records change, and every figure here should be read as of that window. Every vendor assessed has an individual scorecard, available privately and free of charge to that vendor on request, with a standing invitation to correct anything inaccurate: AssessedOnFaith@l4is.ai. No vendor is named in any public version of these findings alongside its own results. A company appears by name only where that company published something itself — a trust page, a disclosure route, a sub-processor list — and then as credit, not as a score.

Cite as: Tubbs, Andrew. Assessed on Faith: Vendor Security Transparency Study. Version 1.0. Level Four LLC, 2026. <https://doi.org/10.5281/zenodo.23600828>

Assessed on Faith — Vendor Security Transparency Study

Published by **Level Four LLC** · l4is.ai · AssessedOnFaith@l4is.ai · DOI 10.5281/zenodo.23600828

DNS and web data collected 5 September 2026. Every assessed brand may request its own scorecard, free and with no commercial ask attached. Corrections to any finding are accepted from anyone at any time and are applied to the dataset.

