Contents

HOLLIS v. PBI - 25CIV60102KCX - MARCH 16, 2026
20-MINUTE ARGUMENT OUTLINE

OPENING - 0 – 2 Min - 2 min

Your Honor, I have a written statement of my case with supporting exhibits, these two copies are **for the court**. Will the defendant be able to see this document during the hearing, or should I have a PDF ready to share?

PBI had **custody** of my Name, Social Security Number, and Date of Birth. Whether they lost my data by throwing it in the trash or via a data breach doesn't matter. They had a duty to protect that information. They **failed**. I spent **3.5 hours** cleaning up their mess. I sent an invoice. They **refused to pay**. That's why we're here.

This is a refiling of case 24CIV19227KCX, which was dismissed because I cannot represent my wife in small claims. This claim is **mine alone**, my data, my time, my remedy. My argument summarizes the document I handed you.

To prevail I need to prove **five elements** under Washington negligence law: Duty, Breach of Duty, Causation, Proximate Cause, and Damages. I'll address each in turn.

<If the judge understands the human story clearly in the first 120 seconds - data lost, remediation done, invoice sent, refused - the rest of the argument is confirmation, not persuasion. Judges who understand the story early tend to read the evidence through that lens.>

1 - DUTY - 2 – 5 Min - 3 min

Duty is the **first element**, and it's the **simplest**.

Washington law, specifically **RCW 19.255.010**, imposes a **duty of care** on any entity that holds personal information. Not just entities that have a contract with you. Any entity that holds your data.

PBI held my Name, Social Security Number, and Date of Birth. That's the **relationship**. • That's the **duty**. •

If there were any doubt about whether PBI believed Washington law applied to them, they **answered it themselves**. After the breach they notified **18,856 Washington State residents** and filed breach notification reports with the Washington State Attorney General. You don't comply with Washington's breach notification statute if you believe you have no obligations to Washington residents. Their **own conduct** confirms they understood the duty.

Courts have consistently recognized this principle. When a company voluntarily assumes custody of individuals' sensitive personal data, a federal court held it may, under the reasoning applied in *McKenzie v. Allconnect*, incur a common-law duty of reasonable care toward those individuals, even in the **absence of a direct contractual relationship**.

PBI may argue they had no direct relationship with me. My answer is straightforward: they had **my data**. That is the relationship the law recognizes. The duty existed the **moment** they took custody of my information.

Notes for delivery:
"That's the relationship. That's the duty.". Dead stop after each sentence. Let it land.
The McKenzie cite, the full citation does not need to be read aloud. "A federal court held" is sufficient. The written record has the full cite.

The last paragraph is the preemptive strike on their primary argument. Deliver it directly, not defensively. This is not anticipating an attack, it is disposing of a known weak argument before it wastes the court's time.

If the judge interrupts and says "but you didn't have a contract with PBI" - that's actually your best moment. "Correct, Your Honor, and Washington law doesn't require one. RCW 19.255.010 applies to any entity holding personal data. PBI demonstrated they knew that when they filed with the Attorney General."

2 - BREACH - 5 – 8 Min - 3 min

Breach of duty is the **second element**. The question is whether PBI's security practices fell below what a reasonably prudent organization should have had in place. The answer is documented in **PBI's own words**.

PBI's public blog, preserved in Appendix E via the Wayback Machine (an organization that archives web pages on The Internet), states that before the breach, their security program consisted of an **annual SOC 2 audit**. SOC 2 is a voluntary compliance standard developed by *accountants*, not *security engineers*. It assesses controls at a **single point in time**. It does not require continuous monitoring. It does *not* mandate multi-factor authentication. It does *not* require penetration testing or network segmentation.
An organization can pass a SOC 2 audit while its operational security is **materially deficient**. That is not a theoretical observation. • That is **what happened here**. •

That blog was publicly accessible until **July 16, 2024** - at which point it was removed. Active litigation over this breach was underway at that time. The **timing is noted**. The content is preserved. It is **in the record**.

After the breach, PBI's own notification letter states they were, per Appendix B, "reviewing and enhancing our information security policies and procedures." Those enhancements were never disclosed by PBI. They were opaque about the specifics. The NIST Cybersecurity Framework, a federal standard freely available since **2014**, prescribes as **baseline controls**: multi-factor authentication, intrusion detection systems, network segmentation, and encryption with proper access controls. These are not advanced measures. They are the floor. Whatever PBI actually implemented, they have confirmed they enhanced their security posture after the breach. From all outward appearances, **they implemented after the fact exactly what a reasonably prudent organization would have had in place before it.**

Your Honor, Appendix B, PBI's breach notification letter, is in the document before you.

Notes for delivery:
"That is not a theoretical observation. It is what happened here.". Same technique as the opening. Short declarative pair. Pause after each.

"Developed by accountants, not security engineers". This is the one moment where my expertise does the work without having to cite my résumé. It reframes SOC 2 for a non-technical judge in one clause.

The blog removal paragraph - deliver it slowly and flatly. No editorial tone. The facts are doing the work. "The timing is noted" lands harder as a neutral statement than as an accusation.

If PBI argues the blog was taken down for unrelated reasons - "I have no way of knowing PBI's reasons. What I know is the dates: active litigation, July 2024, same month. The court can draw its own conclusion."

3 - CAUSATION - 8 – 10.5 Min – 2.5 min

Causation is the **third element**. Washington law requires both cause in fact and proximate cause. I'll address cause in fact here and proximate cause next.

[slowly] The **but-for test** is straightforward. *But for* PBI's breach, my Name, Social Security Number, and Date of Birth would not have been exfiltrated. • *But for* that exfiltration, I would not have spent **3.5 hours** performing the remediation documented in Appendix G. • The causal chain is **direct and uninterrupted**.

The nature of my injury, time spent on protective measures, is **legally recognized** as concrete harm. In *Webb v. Injured Workers Pharmacy*, decided by the **First Circuit Court of Appeals** in 2023, the court held that time spent taking protective measures following a data breach **satisfies the injury requirement**, treating opportunity costs and lost time as equivalent to **monetary injury**. The court specifically distinguished this from speculative future harm - the key factor being that the injury must respond to a **substantial and imminent risk**. Name, Social Security Number, and Date of Birth is precisely the combination required to open fraudulent credit accounts, file false tax returns, and compromise Social Security benefits.

*The risk was not speculative. It was **immediate and ongoing**.*

One additional point. PBI's **own** breach notification letter - Appendix B - instructed me to do **exactly** what I did. Review credit reports. Place credit freezes. Monitor accounts. **I did what PBI told me to do**. The time that consumed is **their liability**, not mine to absorb."

Notes for delivery:
The but-for paragraph - say it slowly. It's three sentences that build a chain. Let the judge follow each link.

Webb - "First Circuit Court of Appeals" is important. This is not not citing a blog post. Federal appellate court. Say it clearly.

"The risk was not speculative. It was immediate and ongoing." - same short declarative technique. This is where I preempting the "no actual fraud occurred" argument without flagging it as a rebuttal.

The last paragraph is the strongest moment in this section. "I did what PBI told me to do" is simple, human, and hard to argue against. Deliver it at normal pace, not rushed.

If PBI argues no actual fraud occurred "Webb directly addresses this, Your Honor. The compensable injury is the time spent on required protective measures, not whether fraud ultimately materialized. The breach created the obligation. I responded to it."

4 - PROXIMATE CAUSE - 10.5 – 12 Min – 1.5 min

Proximate cause is the **fourth element**. The question is whether PBI should have **foreseen** that their security posture could result in exactly this kind of harm.

PBI's defense is that this was a **zero-day vulnerability** - a previously unknown software flaw. They argue that makes the breach *unforeseeable*. That argument **fails on its own logic**. •

Zero-day vulnerabilities are *not* exceptional events. They are the **foundational assumption** of the entire cybersecurity industry. Defense-in-depth exists - the layering of multiple independent controls - precisely *because* any software can be compromised **without warning**. A single-layer security architecture that depends on software protecting itself is *not* a reasonable security posture. It is a **known failure mode**. PBI's own post-breach conduct proves they knew this: they implemented *after* the breach exactly the layered controls they should have had **before** it.

PBI may also argue their data was encrypted, triggering a **safe harbor** under RCW 19.255.010. That argument is **nullified** by PBI's own forensic investigation. Kroll, the firm **PBI hired**, documented that the attackers did not crack PBI's encryption. They used MOVEit's own internal functions to decrypt the data. In plain terms: the door was locked, but **the key was left in the lock**. That is an **architectural failure**, not a safe harbor.

Notes for delivery:
"That argument fails on its own logic" - slight pause after this. This is the explanation for why, and the judge needs to know a turn is coming.

"Known failure mode" - this is the one technical term in this section worth keeping. It's precise, it's damning, and it's accurate.

The encryption paragraph - "the door was locked but the key was left in the lock" is the only analogy in the entire argument. Deliver it conversationally, not dramatically. It should land as obvious, not clever.

Kroll reference - Kroll doesn't need to be explained in detail. "The firm PBI hired" is sufficient and actually makes the point stronger. PBI's own forensic firm documented this.

If PBI argues the zero-day was genuinely unforeseeable - "With respect, Your Honor, that's the point. Zero-days are always unforeseeable in their specifics. That's why every cybersecurity standard requires defense in depth. You build layers because you cannot predict which specific vulnerability will be exploited. PBI didn't. One layer failed and everything was exposed."

5 - DAMAGES - 12 – 15 Min - 3 min

Damages is the **fifth and final element**. My damages are **concrete, documented**, and directly caused by PBI's breach.

On **July 14, 2023** I received PBI's breach notification letter. I immediately recognized the severity. Name, Social Security Number, and Date of Birth is the **maximum-impact combination** for identity theft. It is everything needed to open fraudulent credit accounts, file false tax returns, and **take over a Social Security account**.

[slowly]

I documented my time in **Appendix G**. I spent approximately **one hour** researching the breach and understanding the exposure. **One hour** reviewing credit reports for myself and my wife across all three national credit bureaus - Experian, TransUnion, and Equifax. And **one and a half hours** establishing accounts and placing credit freezes across all three bureaus for both of us. **Three and a half hours total**. Securing only my own accounts while leaving my wife's exposed would have been incomplete remediation as our financial lives are intertwined, and a fraudulent account opened in her name affects my credit, my household, and my financial security just as directly as one opened in mine.

The applicable rate is **$300 per hour**. I have worked in technology for **forty years**. Eleven of those years were specifically in **cybersecurity**, including at Microsoft's Cyber Defense Operations Center where I investigated compromised systems. I secured industrial data centers and SCADA systems supporting the **national electrical grid**, and trained engineers on security hardening. $300 per hour is a **conservative** published rate for a senior cybersecurity consultant in the Seattle metropolitan area. I am not asking for my actual market rate. I am asking for a number **well within** the documented range for this level of expertise.

3.5 hours at $300 per hour is $1,050. That is what I am asking for.

One additional point on damages. Washington law required PBI to notify me within 30 days of discovering the breach. They discovered it no later than **June 3rd, 2023** - the date they reported it to federal law enforcement. My notification letter is dated **July 14th, 2023**. That is **42 days**. *Twelve days* past the statutory limit. For those eleven additional days my most sensitive personal data was exposed while I had **no ability to take protective action**. That delay is documented, it is a **statutory violation**, and it **compounds every element of harm** I have described.

Notes for delivery:
The time breakdown paragraph - slow down here. The judge is following the math. Research, review, freeze. One hour, one hour, one and a half hours. Let each item register before moving to the next.

Credentials paragraph - this is the one time the credentials are stated directly. Deliver it matter-of-factly, not proudly. This is just justifying a number, not auditioning. End it with "$300 is conservative" and move immediately to the total. Don't linger on the resume.

"3.5 hours at $300 per hour is $1,050" - say the math out loud even though it's obvious. Judges appreciate when plaintiffs state their ask with precision.

The notification violation paragraph - this is the final damages point, not a new argument. Frame it as compounding, not as a separate claim. "Compounds every element of harm" ties it back to everything already established.

If PBI argues $300 is inflated - "Your Honor, I am not asking for my top market rate. $300 is a conservative figure for a senior cybersecurity professional in the Seattle area. If PBI had hired a consultant to perform this remediation, they would have paid at least that rate. Instead I absorbed that cost because of their negligence."

If PBI argues the time is inflated or unverifiable - "The steps are documented in Appendix G and they are exactly the steps PBI's own breach notification letter instructed affected individuals to take. I did what they told me to do. The three credit bureaus deliberately make this process time-consuming. Anyone who has done it knows that."

CLOSING - 15 – 17 Min - 2 min

Your Honor, I'll summarize. •

PBI held my **most sensitive personal information**. They lost it due to security practices that fell below every recognized industry standard. Their **own** post-breach conduct confirms what those standards required. Their **own** deleted blog confirms what they had in place before the breach. Their **own** forensic firm documented how the data was taken.

They notified me **41 days** after they knew - *in violation of Washington law*. For those 41 days my data was in the hands of threat actors while I had **no ability to respond**.

When I finally received their letter, I did **exactly** what they told me to do. **I spent 3.5 hours** of specialized professional time cleaning up their mess. **I documented it.** I **invoiced them**. They **refused to pay**. •

Washington law recognizes that time spent on required protective measures following a data breach is a **concrete, compensable injury**. I am not asking for a windfall. I am asking to be made whole for **3.5 hours** of documented work I would never have performed but for PBI's negligence.

I am asking the court to award me $1,050. •

Notes for delivery:
Stop after "I'll summarize." Full stop. Let the room settle. Then begin.
"Their own post-breach conduct. Their own deleted blog. Their own forensic firm." - the triple parallel is intentional. Each one lands harder than the last because it's all PBI's own evidence convicting them.
"I documented it. I invoiced them. They refused to pay." - same technique. Three short sentences. Don't rush the last one.
The final two paragraphs are the ask. Drop the pace noticeably. "$1,050" is the last number the judge hears. Say it clearly and then stop talking.
After "the court to award me $1,050"- do not fill the silence. Do not add "thank you" or "that's all I have." Stop at $1,050 and wait for the judge. The instinct to keep talking after a closing is almost universal and almost always wrong. Resist it.

Big picture
There are several things in my favor:

- Very clear, concrete harm (3.5 documented hours, modest rate, modest total).
- A straightforward story: “They lost my data; I did the work they told me to do; they won’t pay.”
- Anchoring in Washington statutes + one very on-point persuasive case (Webb).

What cuts against:

- Washington small-claims judges vary a lot on how receptive they are to “time as damages” without out-of-pocket loss.
- Defense will argue: “no contract, no out-of-pocket payment, no actual identity theft, and no Washington case saying you can get paid for your time alone.”
- Defense will also argue the document repeatedly references Rose in the remediation context; they don't want to pay for her "My wife's data was also compromised. I am claiming my time regardless of whose account was being secured during that time - Webb v. IWP directly addresses this."

It is a real chance; it’s not a slam dunk, but the odds are much better with this outline than a typical pro se data-breach claim.
Time-management and strategy tips

- **Don’t overstuff the 20 minutes.** Aim for 15–17 minutes of material so there is room for questions. If the judge interrupts with questions, answer them directly, then return to the outline.
- **Prioritize story + damages.** If you have to cut time, cut from the deep technical discussion and keep: opening, causation, damages, closing.
- **Be ready with one-sentence “pivots”:**
    - If the judge asks “Why is this more than just inconvenience?” → “Because it is three and a half hours of specialized work that I would never have done but for their breach, and that time has real value.”
    - If the judge says “I don’t see Washington cases on this” → “That’s right, Your Honor; this is an area where Washington law is still developing. That’s why I’ve pointed to persuasive federal cases that treat time spent on mandatory remedial steps as a real injury.”

IF PBI ARGUES	The response (short)
No duty / no relationship	"Washington law imposes duties on any entity that holds personal information. RCW 19.255.010 doesn't require a contract with me; they held my data, that's enough."
Zero-day = unforeseeable	"Zero-days are *why* you build defense in depth. You assume software will have unknown flaws and you add layers so one flaw doesn't expose everything."
Encryption safe harbor	"The attackers used MOVEit's own decryption functions. When your own system decrypts data for the attacker, the encryption safe harbor doesn't make sense in practice."
No actual fraud occurred	"The harm here is the time I had to spend on required protective steps. Courts, including the Webb case, recognize that remediation time itself is a concrete injury, even before fraud happens."
No out-of-pocket loss / no WA case on time-only damages	"My loss is three and a half hours of specialized work that I would not have done but for their breach. There may not yet be a Washington case on this specific point, but other courts have treated that lost time as compensable, and small-claims is designed to resolve exactly these kinds of practical harms."
Jurisdiction	"This court has already denied their jurisdiction arguments. I'm not asking the Court to revisit that today."
Stay for class action	"My claim is for my own individual, documented time. Whatever happens in class actions, I'm entitled to pursue my own remedy here."

Memorize the *idea* in each response, keep it conversational and adjust to how the judge phrases the question, rather than sounding like it is reading a script.

Industry experience helps, but in a specific, limited way.

How it helps

- **Justifying the hourly rate:**
  40 years in tech and 11 years in cybersecurity (including Microsoft, CDOC, SCADA/ICS, critical infrastructure) make 300$/hour sound reasonable rather than inflated. It makes it easier for the judge to accept that the time genuinely has that market value.
- **Explaining why the time was necessary:**
  Credibly describe the remediation steps as *necessary and proportionate* to the risk, not overkill. That counters any argument that I "over-reacted" or did unnecessary work.
- **Framing as a careful, informed plaintiff:**
  Come across as someone who understands security and didn't manufacture work. That can increase the judge's comfort that the 3.5 hours logged are real and not exaggerated.

How it doesn’t help

- It does **not** create a special legal right to be paid just because of the high skills. The judge still has to be persuaded that:
    1. the time was reasonably caused by PBI’s breach, and
    2. time alone is a compensable harm in this context.
- Don't lean too hard on the resume, a skeptical judge might think “This sounds like expert-witness testimony in a small-claims case,” which can backfire.

How to use it in argument

- Keep it tight and functional:
    - “I’ve worked in technology for about forty years, and in cybersecurity for about eleven, including at Microsoft. Based on that experience, the steps I took were the minimum needed to reduce the risk from this breach.”
    - “A 300$/hour rate is conservative for that level of experience in this field.”
- Then pivot back to the simple ask:
    - “So I’m not speculating about the risk or inflating my time; I did exactly what needed to be done, and I’m asking to be compensated for that 3.5 hours.”