Slide 1



July 2023. A letter shows up from a company I'd never heard of and never done business with directly. Pension Benefit Information. They wanted me to know they'd lost my name, Social Security number, and date of birth - and my wife's.

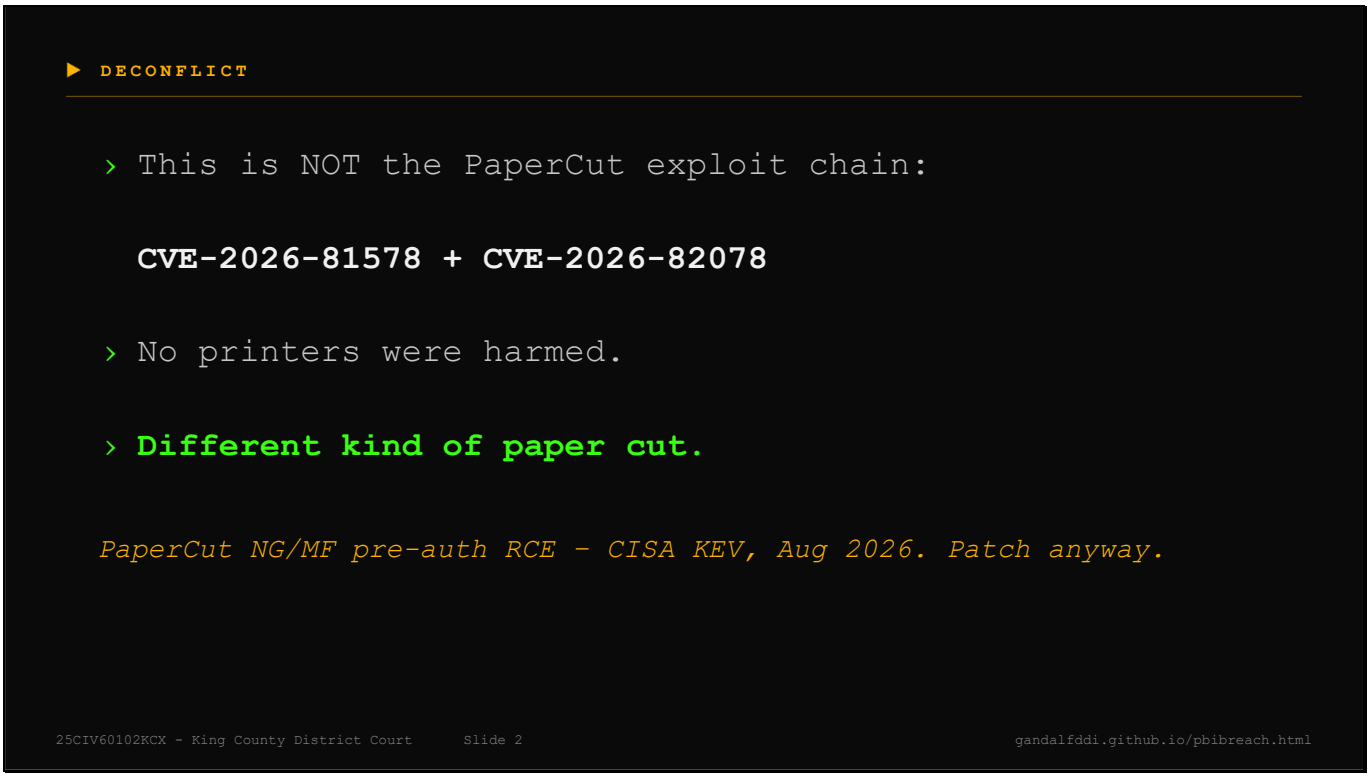
Show of hands, who got a "your data was compromised ... Oops" letter? [pause] Yeah.

Of course I started digging the minute I opened it. You would too. Between the letter, what was public about the MOVEit vulnerability mentioned in the letter (Thank you Kroll for expounding), and my years in Microsoft's Cyber Defense Operations Center, I filled in the parts they weren't saying.

The more I dug, the more annoyed I got. I was spending my personal time cleaning up their mess and having to deal with the three credit services Equifax, Transunion, and Experian.

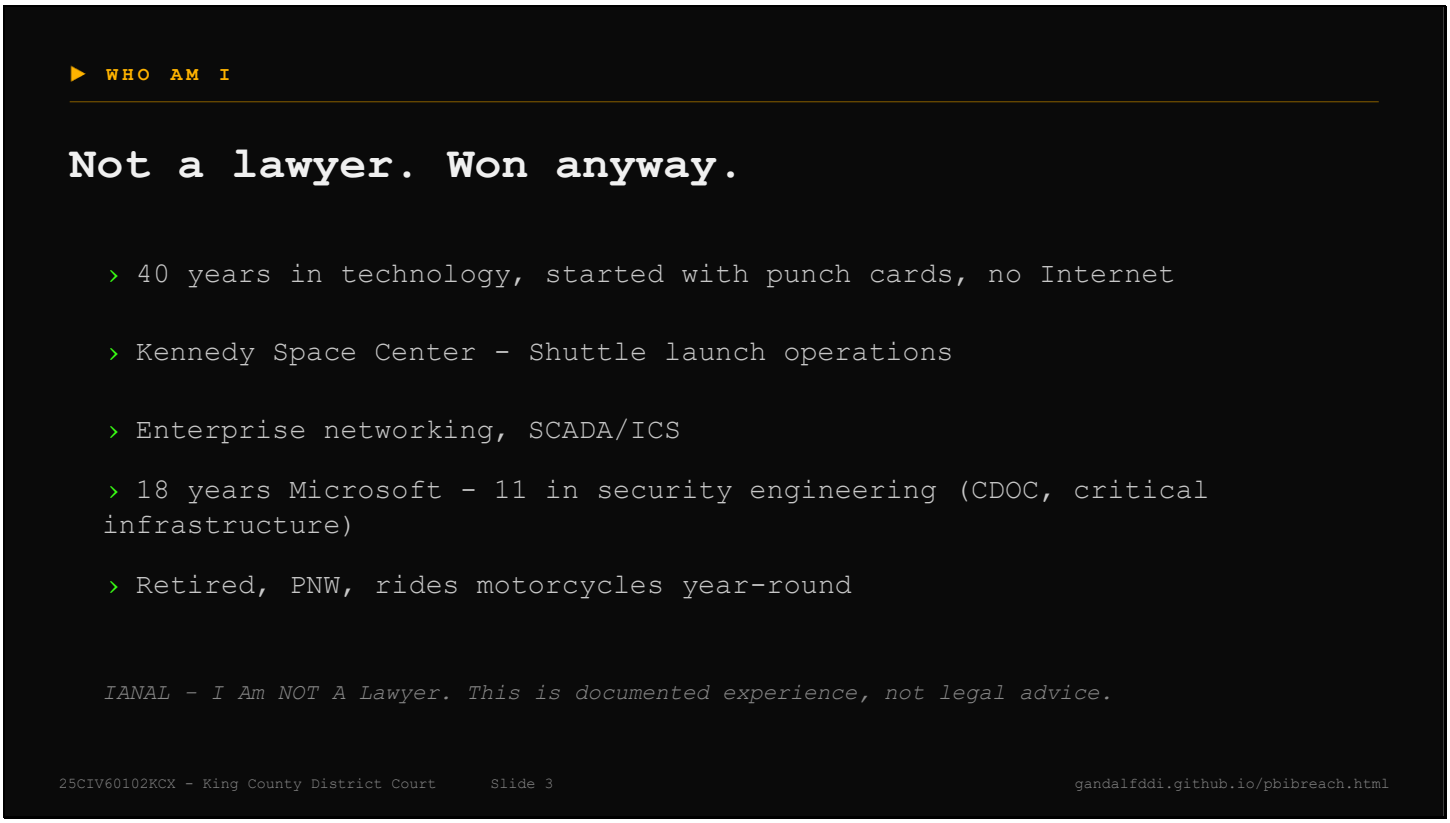
I made mistakes along the way. You get them for free today. And in the end, I made them pay for my time ... one hour of it anyway, plus it cost them a lawyer's time (multiple hours) and their CEO's day in court to lose.

Slide 2



This talk is NOT about the late Aug 2026 PaperCut CVE. Half this room patched your PaperCut NG and PaperCut MF software. The rest of you NEED to patch. ☺ Different paper cut.

Slide 3

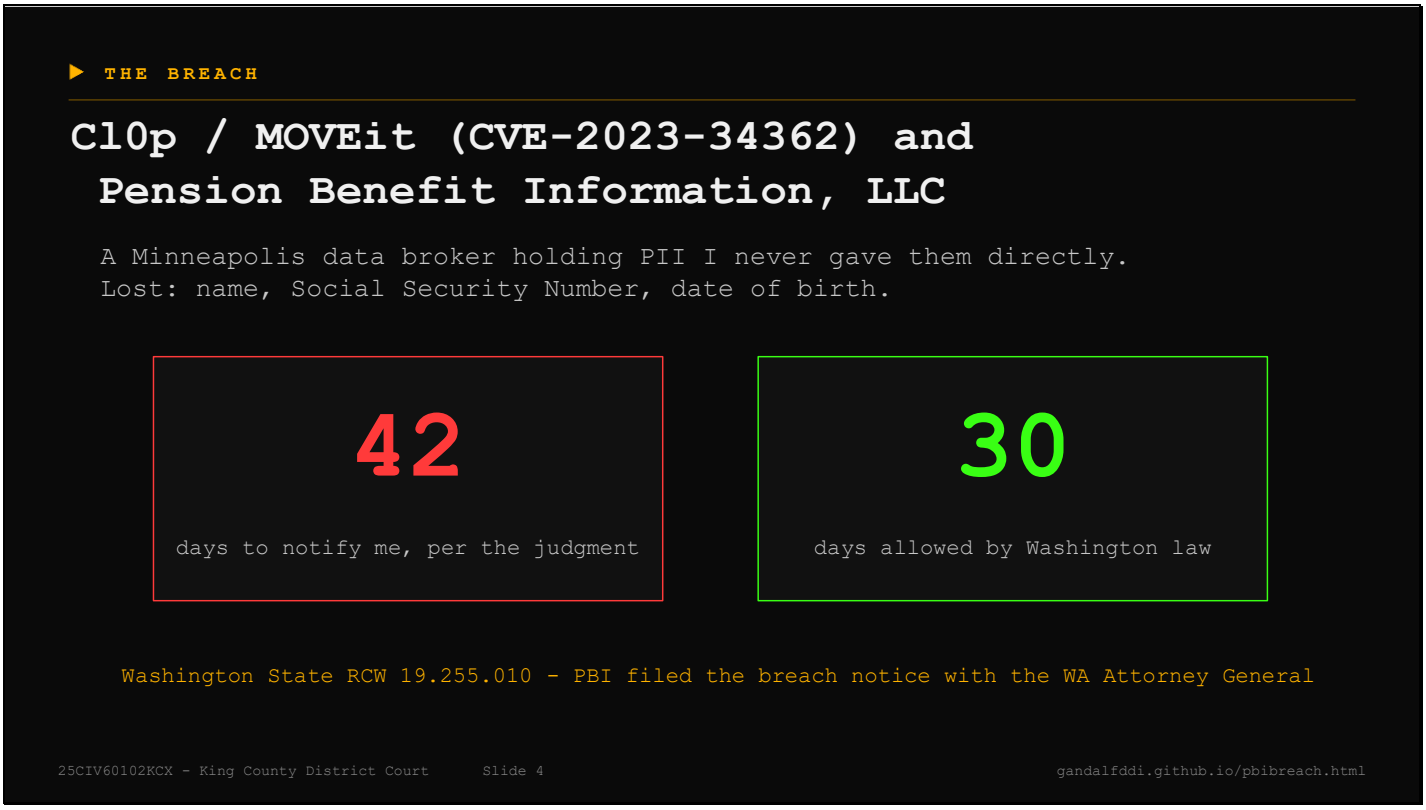


IANAL. Just persistent, like many of you. What REALLY got me into all of this was their assumption that I would work for them for free because they had bad cybersecurity. In the end companies just care about if they are legally covered, no care about the customers that were compromised. " We take the security of your information very seriously" Yeah. Sure you do. Thoughts & prayers

Honestly the one advantage I had: time. I was retired by the time this got to court and I could dig into the legal aspects. Hopefully this paper will save you some time. Letter in July 2023. Invoice that August. First filing in 2024 which was dismissed. Refiled in 2025. Trial in March 2026. Almost three years from letter to check.

Court doesn't happen on your schedule. Pretrial hearing was a weekday at 8:45 in the morning. The court decides if it is in person or videoconference, but it is mandatory. Then mediation. Then trial. If you're working, plan for the time off, that is part of what this costs you. It's not a weekend project, it's a slow burn. Persistence is the whole strategy and how you wear down the other side.

Slide 4



Cl0p – Russian-speaking ransomware and extortion gang also known as Lace Tempest. For MOVEit they didn't bother encrypting anything. Smash-and-grab, steal the data, post the victims on a leak site, demand payment. Cl0p apparently sat on this exploit for 2 years then picked the right moment to exploit, probably running scans & targeting vulnerable companies that had data they wanted.

CVE-2023-34362, a SQL injection in Progress Software's MOVEit Transfer. A file-transfer tool companies use to move sensitive data. It was disclosed May 31, 2023. Cl0p was already in, exploiting it over Memorial Day weekend – a holiday weekend, naturally.

The damage: About 93 million people and greater than 2,700 organizations. A lot of you are probably in that number. I was. That's how I got here. The 42 days PBI took to notify me was 42 days my data was exposed without me knowing



I did what any consultant does. I sent them a bill. You MUST send an invoice. This is the first step, it creates the refusal, and the refusal is the story a judge understands instantly.

The answer came back from "PBI Research Services", their trade name, not their legal name. Remember that; it matters later. "Due to pending litigation ... PBI is not engaging in negotiations with individuals at this time.".



I then looked at small claims. Turns out it's the people's court, lawyers can't even appear unless the judge allows it. I sued them in small claims court for $1,050. PBI showed up with corporate counsel and a motion to dismiss. That right there cost them more than the $1,050 I was asking for. Washington state you have three years to file a small claims case, Oregon is 2 years from what I can tell.

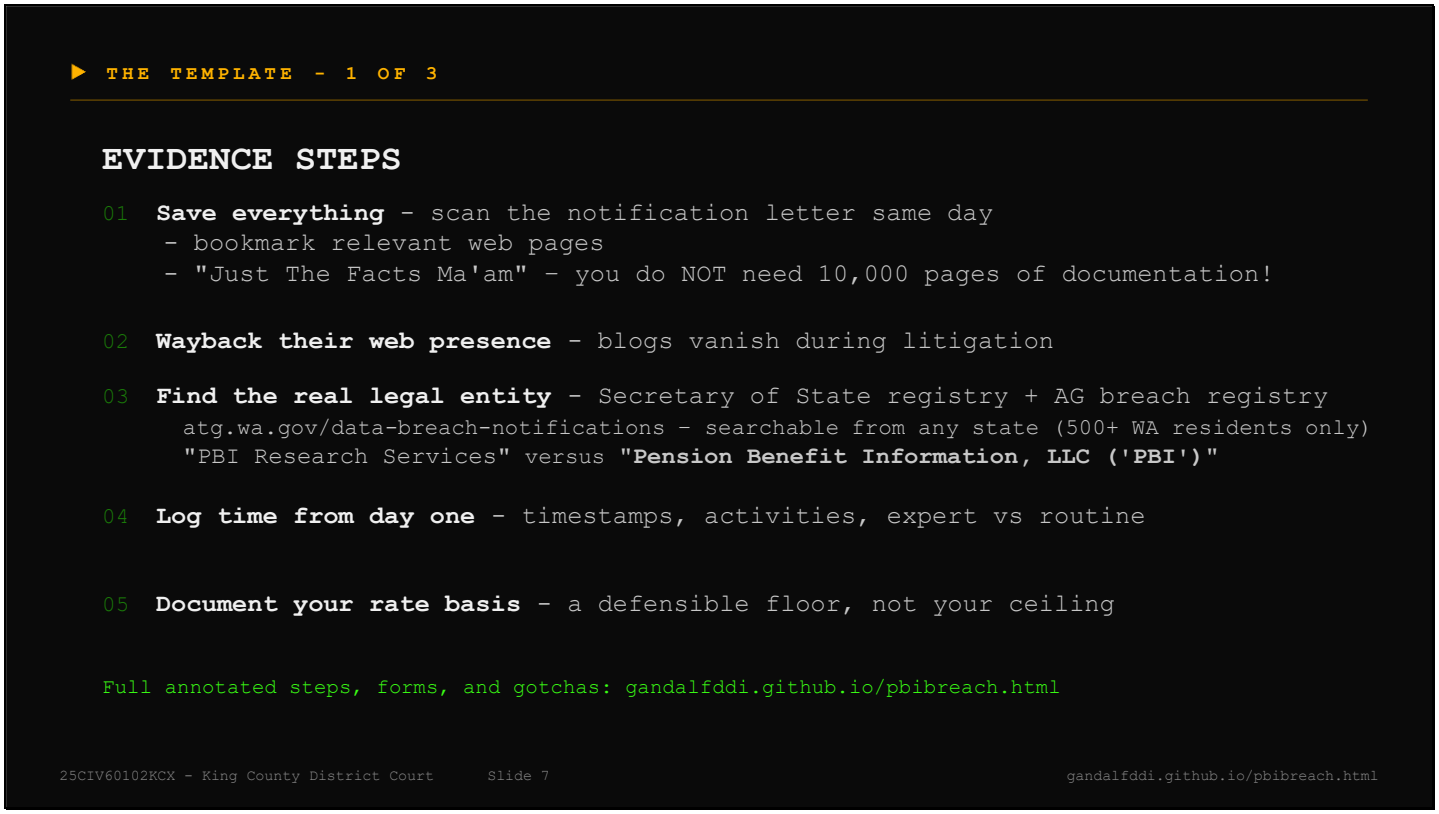
PBI lawyer raised that I should just join the class action suit. From the addendum: "PBI points to the fact that there are large-scale class action lawsuits pending, including against PBI." The judge didn't buy it: "potential class members are entitled to opt out of the class by filing their own lawsuit. That is what Hollis has done." I didn't even have to argue it – the judge did it for me.

You can do Small Claims OR Class Action, not both.

If you got a breach letter, you're in the class by default – nobody asks you. Lawyers file on behalf of everyone and typically take a quarter to a third off the top. Your share: a few dollars and another round of credit monitoring. When a settlement notice arrives, it has an opt-out deadline. Miss it and you're bound by the settlement – including the release that says you can't sue them yourself.

They offer "free credit monitoring" but the problem is that it tells you after someone opens an account in your name, too late. A freeze stops them from opening it. Freezes are free. Your SSN doesn't expire in two years – unlike the credit monitoring that does expire.

Slide 7



These are the steps and some of my mistakes

Step 1. KISS – Keep It Super Simple. Don't muddy the waters; just the pages that prove your points. I found a page from an "industry solution provider" making claims with no solid reference, it stayed out of my evidence.

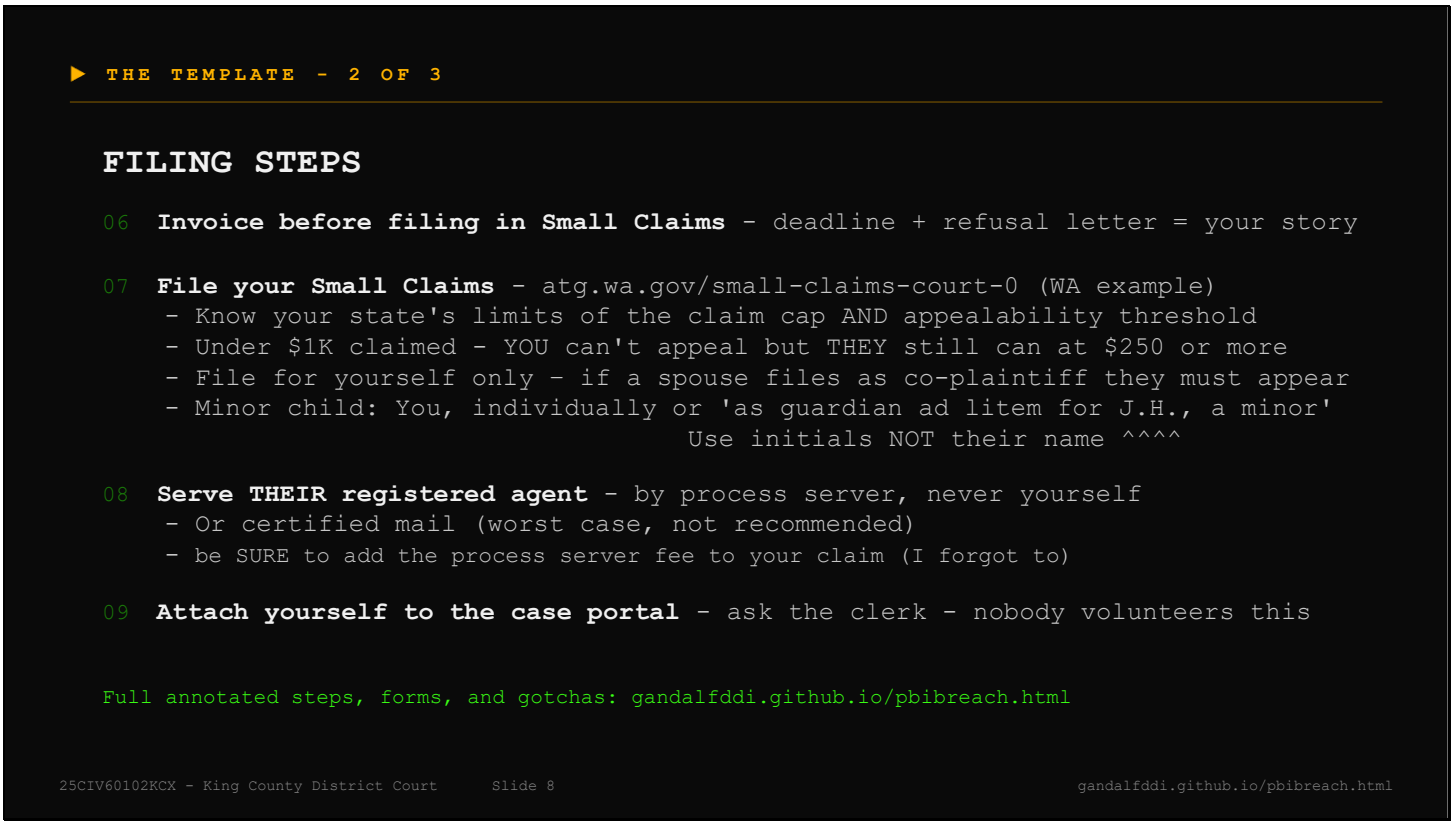
Step 2 – PBI's blog described their security program. It disappeared on July 16, 2024 while litigation was underway. Luckily the Wayback Machine already had it. It's in my evidence. Keep copies locally of anything the day you get the letter, it may disappear later.

Their own blog (which was later deleted) discussed an annual SOC 2 audit. If you've lived through one, you just winced. The company, not the auditors, write their own checklist. An auditor confirms they followed the checklist that they wrote. No MFA, no pentest, no network segmentation required unless they call it out.

Step 3 – PBI used two names: "PBI Research Services" and "Pension Benefit Information, LLC." Only one is the legal entity (the LLC). Sue the legal entity. Read the fine print. I didn't & I had to correct the Small Claims case and pay a Process Sever twice.

Step 4 – Split expert time from routine time from day one. The judge did it for me anyway, one hour paid, the credit freezes were unpaid.

Step 5 – I asked for $300 an hour, a conservative rate for my field and area. The judge accepted exactly that. Ask for your floor, not your ceiling.

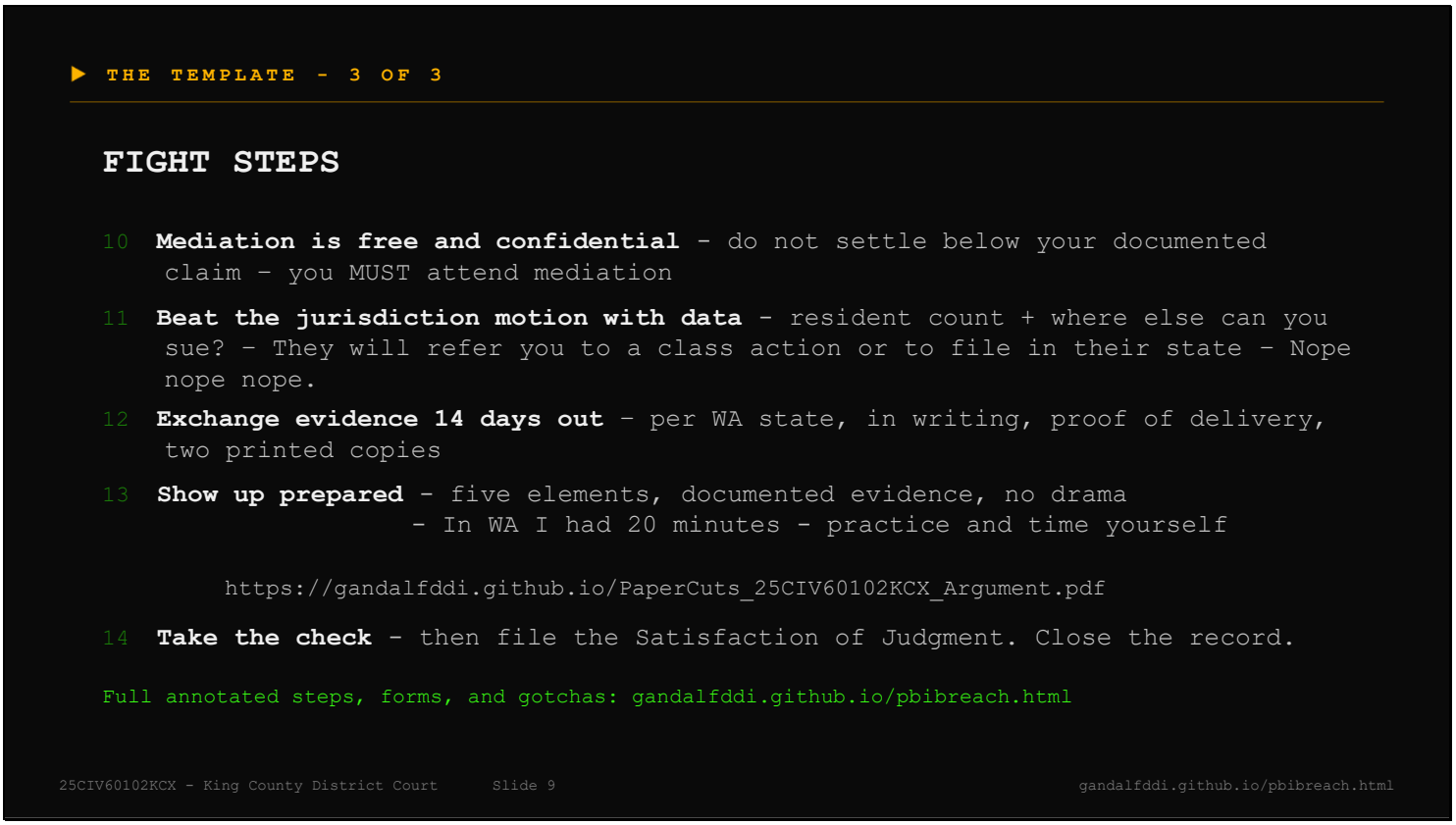


Step 6 – Invoice first. The refusal letter is your whole story in two seconds.

Step 7 – My first filing was for my wife's claim. You can't represent anyone but yourself in small claims and it was dismissed. I had to refile for myself. If your spouse wants in, they file as co-plaintiff and show up to every hearing. Adult kids file for themselves. For a minor you file in your own name, or the court appoints you guardian ad litem.
Washington: claim under $1,000 and YOU can't appeal, THEY still can at $250 or more. Know that before you pick your number.

Step 8 – Service of process will bite you. A non-party over 18 serves them, never you. Hire a professional process server in the registered agent's city. Process servers do this every day; your cousin doesn't.
Washington: served at least 10 days before pretrial, Declaration of Service filed. Miss it and you're done.
Certified mail? Only counts if the right person signs – and they can refuse. Don't use Certified Mail. Add the process server fee to your claim. I didn't – about $80 per delivery, my bad.

Step 9 – After you file, ask the clerk how to attach yourself to the case portal. It's not automatic and nobody tells you.



Step 10 – Mediation. Mandatory, free, confidential. If they low-ball you, walk. It costs nothing extra to go to trial if the number is wrong. If you're feeling generous, offer some basic cybersecurity training for their staff. They'll probably refuse.

Before mediation, their lawyer may want a "just want to chat" call "maybe we can work this out before mediation." This is NOT a friendly call. That call isn't mediation, what you say can be used … They're fishing for something to use against you. Be polite, be brief, and save it for mediation.

Their C-suite (Corporate Executive Suite) doesn't want a judgment on the record, and they really don't want the rest of you doing this. Which is exactly why I'm up here 😊.

Step 11 – The jurisdiction motion – we will discuss that soon. Stay calm, your state, their numbers they have already stated of how many people in your state were affected.

Step 12 – Exchange evidence 14 days before trial, in writing, with proof of delivery. Two printed copies in the courtroom – the clerk doesn't make copies for the judge.

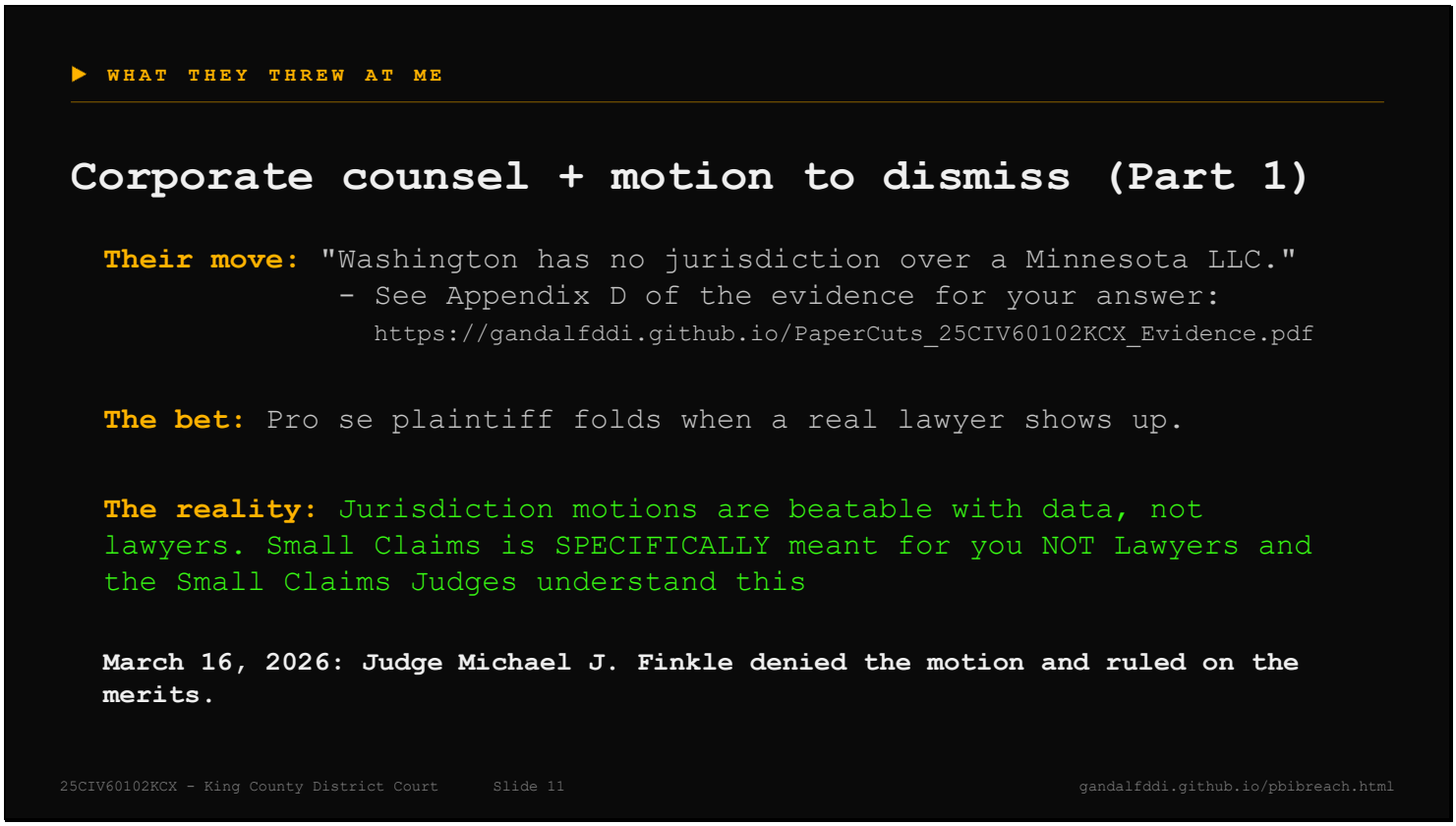
Step 13 – Show up prepared. Five elements: duty, breach, causation, proximate cause, damages. My full argument outline is on the site. Copy, paste & update as necessary. I had 20 minutes for my argument(s).

Step 14 – Take the check. File the Satisfaction of Judgment and close the record.

Slide 10



These are the rules for Oregon, read it yourself, I am describing what I read and have NOT been through the Oregon small claims, YMMV. Oregon small claims caps at $10,000 and keeps lawyers out unless the judge allows one. My $1,050 claim could have resulted in a jury in Oregon, obviously keep an Oregon claim at $750 or under per your time logs.



Do not be intimidated by opposing counsel appearing. The playbook gives you rebuttals. The lawyers just want you to be intimidated & to go away. See the Evidence example for legal rebuttals.

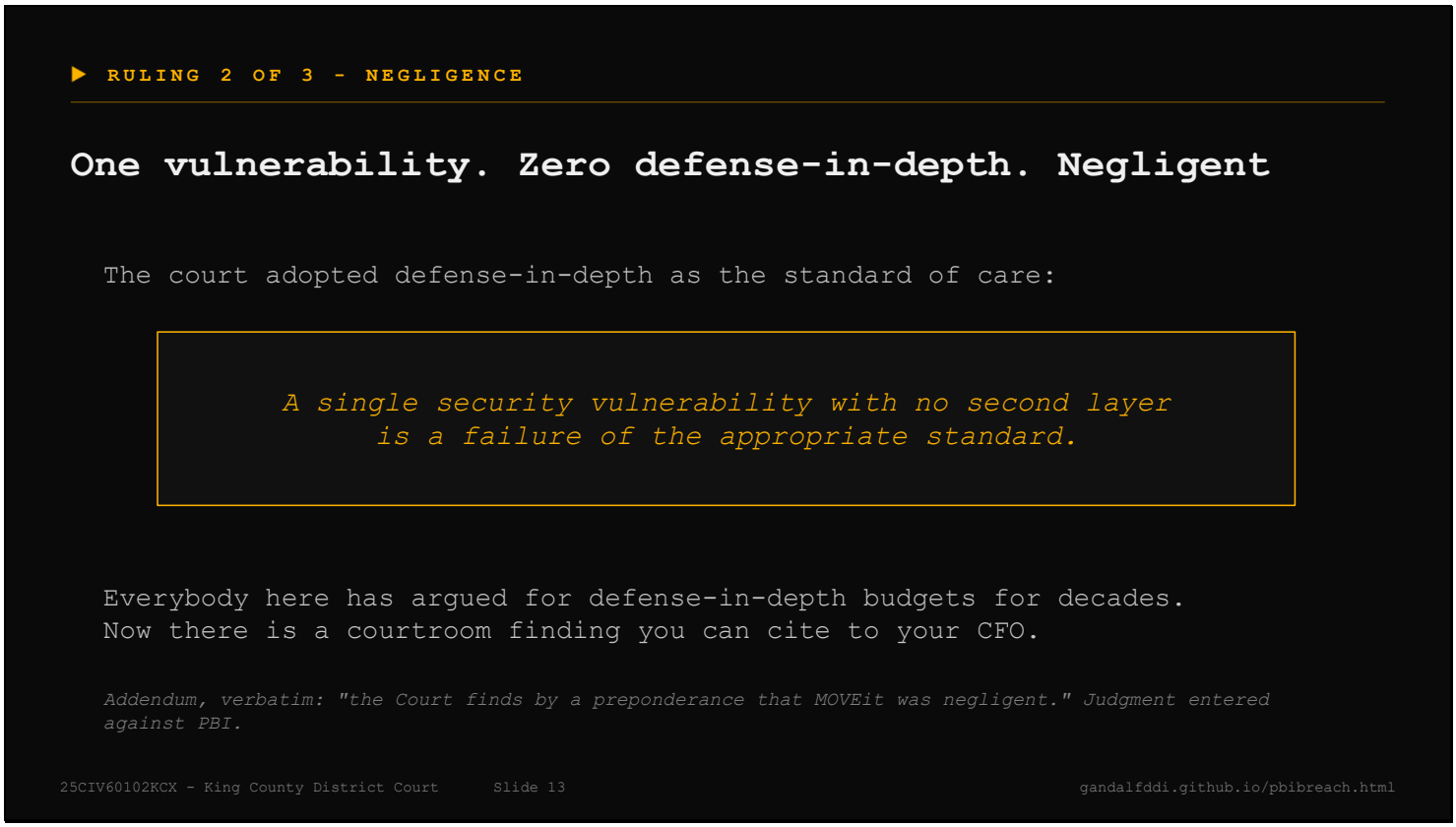


Stay calm. When a corporate lawyer files a motion to dismiss, it's designed to make you fold. Don't.

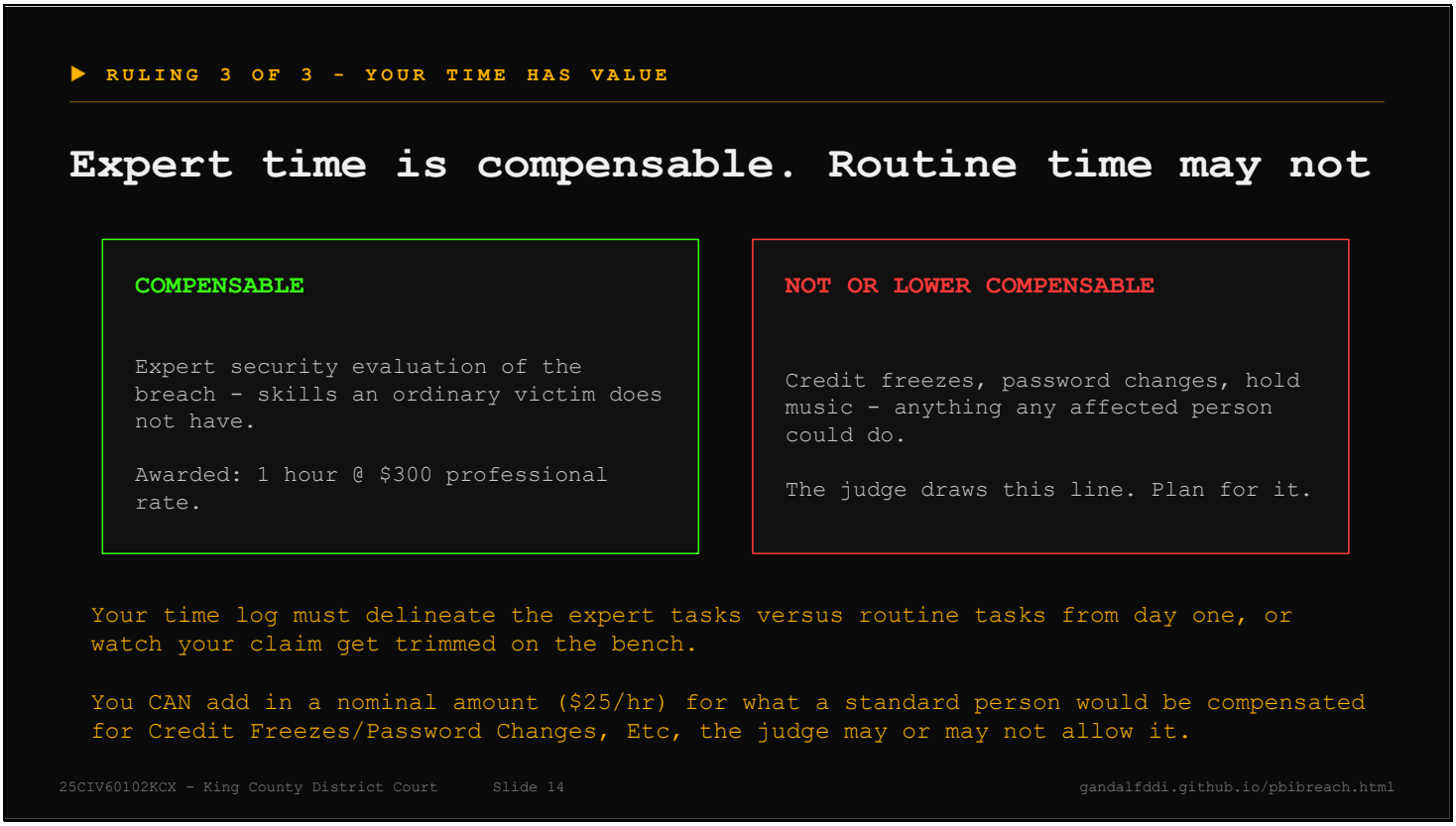
Your state, your court. They held your data, the harm landed here, and you live here.

PBI filed breach notices with the Washington Attorney General for almost 19,000 Washington residents. PBI's lawyer added a line saying that notice didn't concede jurisdiction. Fine. It still proves they knew they held Washington resident data and were subject to the laws of Washington. Their number, not yours. And you are not alone. Where else can those 19,000 people practically sue? Minnesota? Drive there? The judge's answer was: here in Washington State.

Don't throw everything into your argument. Just the salient facts. Resident count. Where else can they sue. Their own filing as your exhibit. Just the facts, ma'am.



Small claims is not a binding precedent, and a judge hearing YOUR case may or may not find this ruling useful - some judges will read it with interest, some will shrug. The playbook is what is important, not my ruling: your documentation and your own state's negligence and notification statutes. My example proves the path exists; BUT every case still walks it on its own facts. ***"The Court finds by a preponderance that MOVEit was negligent." With a judgment entered against PBI.***



Professional skills change what your time is worth in court. Your time for doing non-professional activities may be less … Or zero. No harm in asking for it.



"Only $350?". Yes, but if EACH ONE of us did that think of the time (ESPECIALLY legal time) and money the negligent companies would spend on each case. Multiply by the affected-resident count and the economics of negligence change. Another lesson: know the appeal rules BEFORE you pick your claim amount. In Washington, claiming under $1,000 only takes away MY right to appeal, they can still appeal anything $250 or more. In Oregon, keep it at $750 or under so they can't demand a jury. Check the limits in your state, otherwise it could get more complicated.



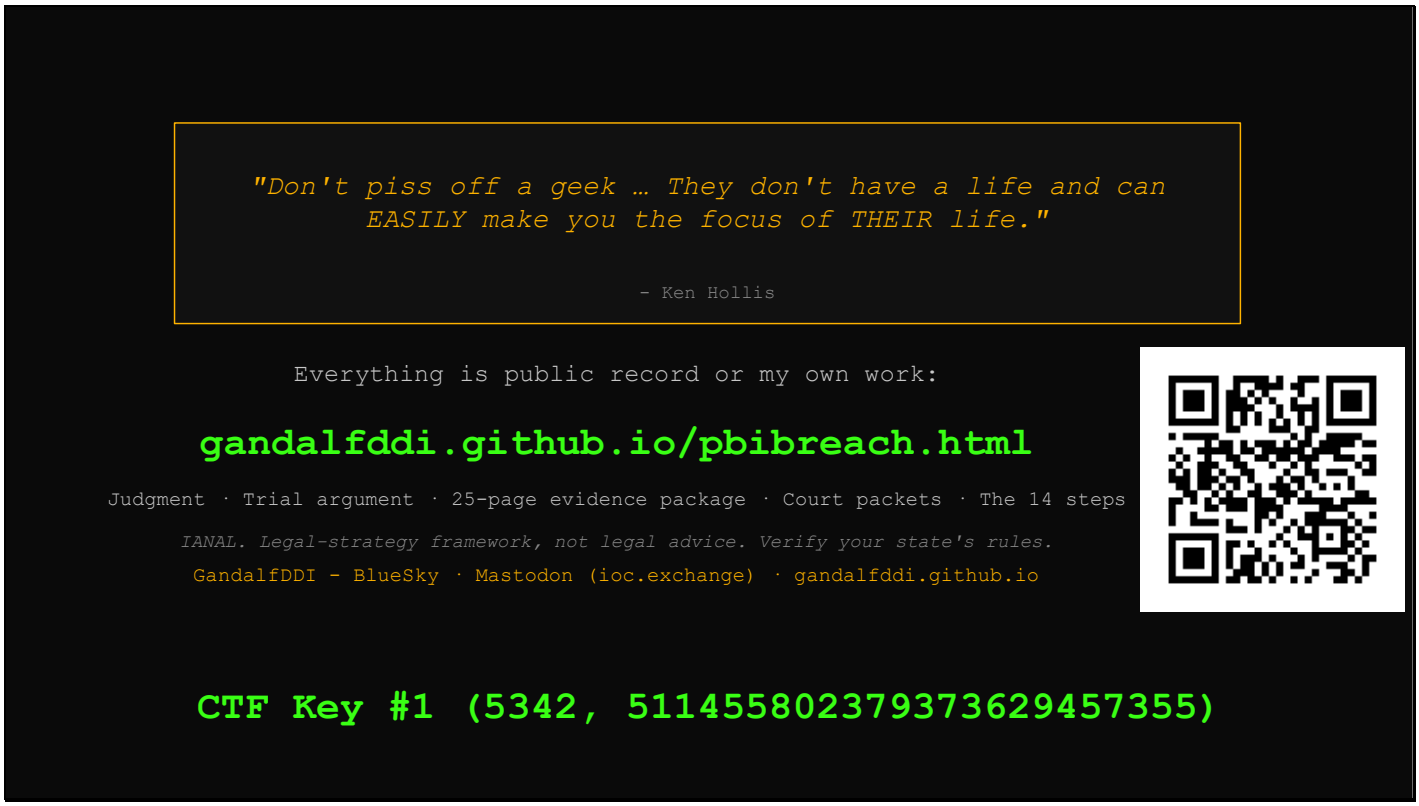
The barrier was never lawyers. You already keep logs, versions, evidence, and write postmortems. Those ARE the skills. You can do this in your sleep.

NOW you have the Small Claims workflow. Find the real legal entity. Log expert time separately from routine time. Invoice first. Serve the registered agent – never yourself. Fourteen steps, all on the site.

The lawyers will try to bluff you out of it. They're betting you'll fold. Don't.

Next time a breach letter shows up – and it will – start the clock the day you open the letter

Slide 17



This is the URL - gandalfddi.github.io/pbibreach.html - with all the information. Precedent: small claims binds nobody, and another judge may or may not care what this one found - the method replicates, the ruling does not. That is enough.

Questions???