UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

In re: Target Corporation Customer Data Security Breach Litigation,	)	File No. MDL 14-2522 (PAM/JJK)
This transcript relates to: Financial Institution Cases.	)	St. Paul, Minnesota September 10, 2015 10:00 a.m.

BEFORE THE HONORABLE PAUL A. MAGNUSON
UNITED STATES DISTRICT COURT JUDGE
(HEARING ON CLASS CERTIFICATION)

APPEARANCES

For the Plaintiffs:	**ZIMMERMAN REED, PLLP** **CHARLES ZIMMERMAN, ESQ.** **BRIAN GUDMUNDSON, ESQ.** **J. GORDON RUDD, JR., ESQ.** **DAVID CIALKOWSKI, ESQ.** 651 Nicollet Mall, #501 Minneapolis, Minnesota 55402
	CHESTNUT CAMBRONNE, P.A. **KARL CAMBRONNE, ESQ.** 17 Washington Ave. N., #300 Minneapolis, Minnesota 55401
For Defendant Target Corporation:	**FAEGRE, BAKER, DANIELS, LLP** **WENDY WILDUNG, ESQ.** 90 S. 7th St., #2200 Minneapolis, Minnesota 55402
	ROPES & GRAY, LLP **DOUGLAS MEAL, ESQ.** **MICHELLE VISSER, ESQ.** **RICHARD BATCHELDER, ESQ.** Prudential Tower 800 Boylston St. Boston, Massachusetts 02199
Court Reporter:	DEBRA BEAUVAIS, RPR-CRR 300 S. 4th St., #1005 Minneapolis, Minnesota 55415

Proceedings recorded by mechanical stenography; transcript produced by computer.

P R O C E E D I N G S

IN OPEN COURT

THE LAW CLERK: All rise. United States District Court for the District of Minnesota is now in session, the Honorable Paul A. Magnuson presiding.

Please be seated.

THE COURT: Good morning, everybody. We've got the Target Consumer Data Security Breach litigation matter Motion For Class Certification.

I realize that I put some kind of tight time restrictions on you, so I'm not going to ask you a lot of questions, just let you put your best foot forward on it.

Mr. Cambronne, you're sitting on the front seat, so I assume you're going to stand up.

MR. CAMBRONNE: I will stand up, Your Honor.

Your Honor, kind of distilling to what I think is its essence is defendant acts that facts and law do not predominate and hence you should not be thinking about certifying a (b)(3) class. Your Honor, at this stage of the litigation, we have developed facts that are no longer just the allegations of a complaint. And we can prove, we believe, both liability and damages using common proof, which satisfies that requisite of Rule 23.

In order to assist Your Honor, I have put up on the screen, but also shared with counsel, a timeline that

will, I think, be helpful to the Court in understanding why we are confident that we can prove this case, liability and damages, using common proof.

Prior to the breach, Your Honor, that happened essentially December of 2013, earlier that year, Target had received a number of warnings from internal sources, from outside sources like Deloitte and Visa, that said there is a new malware out there that if it infects your point of sale or POS terminals, it can scrape card data, all the information on the magnetic stripe, thereby compromising those cards. That was important and well-publicized, and Target knew it.

Target then in October of 2013 installed what's called the FireEye system, Your Honor. Importantly, though, that FireEye system, although very, very efficient and does do its trick, and can and does discover the existence of malware on a computer system, that installation was in a detection mode only, not a scrub mode. In other words, what that means, Your Honor, is that Target had available to it in October of 2013 an ability to make sure that if it was infected by this vastly warned against malware called BlackPOS, it could not only identify it but eliminate it, no harm no foul, eventually no lawsuit. But they had turned that off, Your Honor, for reasons nobody at Target has been yet willing to tell us.

And then Target -- number two up there, Your Honor -- did something that is interesting but is not unusual for a merchant. It instituted a computer system "freeze" at its organization over in Minneapolis there. And what that meant is changes to the system could not be internally generated at Target because they didn't want to interrupt the important, we all acknowledge, Christmas holiday shopping season. So what it did, that "freeze," is make fixes impossible to accomplish.

Some time during the last two weeks of November, Your Honor, what was warned against did, indeed, happen -- that is, malware was put on the point of sale cash registers at Target across the nation.

Now, it's interesting to note that this information, this ability to hack, if you will, the computer system at Target was accomplished through using the credentials of a third-party vendor out in Pennsylvania, a heating and air conditioning company. But once they got into the Fazio -- that's with a Z -- system out there they could, the hacker, gain access completely and fully to the Target computer system. Everything that happened in that company could now be known to outside persons.

With that portal opened, if you will, Your Honor, what happened then was the hacker put this malware that had been warned against, that really Target could have protected

against, was put on the point of sale outlets during the heavy business Christmas season at Target.

Now, we know, Your Honor, that Target learned of this hack through Symantec, which is another software company, back in November also -- that is, it was installed in November '13. It also was discovered by Target back in 2013. We have people in-house saying they're working on it on Thanksgiving Day in 2013.

So we have installation, even though it didn't have to happen, of this malware on the computer system. And during the next two or three weeks, Your Honor, the full information on a magnetic stripe of a credit card was used -- was and could be taken and stored, and it was stored continuously at Target, and that information.

Now, Target being aware of it in late November did eventually remove all this malware, Your Honor, but then the deed had been done. Over 40 million cards the information of consumers had been stripped away and obtained by the bad guys, if you will. And they had that in their arsenal, if you will.

Now, Target publicly disclosed on December 19th that they had been the victim of a hack. That's interesting, Your Honor, because they knew they had been the victim of a hack back in November. But on December 19th is when they chose to disclose the information, Your Honor.

And what happened then, Your Honor, is the deed had been done. The fox was out of the chicken coop, and a hack was disclosed.

Now, credit-card companies on December 20th began telling the banks that issued these cards the following cards have been the subject of an intrusion, a hack if you will, a breach of data at the Target Corporation, and began notifying. In fact, some 90 plus percent of the cards affected and their issuing banks had been notified by December 20th. But then that's when the cat is out of the bag, as I say.

Now the question becomes, and this gets to the issues that I think Target wants to focus on, what happens then. We have full notification to the rest of the world what Target knew for the last three weeks. Targets were notified officially. And the important thing, Your Honor, is that banks had to act. They had to act. Now, that is not just an argument of a lawyer, Your Honor. That is the subject of various laws and expert testimony. And I'll talk to that in a minute, but maybe one reference to the law that supports the notion that banks had to act is the Federal Deposit Insurance Corporation's Financial Institution letter back in 2005, Your Honor, 2005. And this is the guidance on response programs for unauthorized access to customer information and customer notice. So banks know that when

they detect or are advised of a hack of information on the cards that they issue they have to do something. That is part of the Librock deposition, Your Honor. You have it before you in one of the affidavits. But, anyway, I quote just two sentences. This is the FDIC interpreting the Gramm-Leach-Bliley Act, Section 501. It says, At a minimum, an institution's response program should contain procedures for taking appropriate steps to contain and control the incident, to prevent further unauthorized access or to use customer information -- that is, prevent further unauthorized access to or use of customer information. So we have federal law imposing upon banks a need to act. This is something that should be without question, Your Honor. Under the Electronic Funds Transfer Act, banks are responsible to pay fraud charges, not the individual cardholder. Visa rules tell banks they have to act in the face of such information.

So we say -- and this is a common impact, Your Honor -- we say banks had this legal obligation to act. Our expert says they do it because they want to avoid losses, they want to avoid customers getting angry, they want to avoid regulatory backfire from the regulators, and they want to protect their own reputations. So being faced with the need to act banks acted.

Now, it is Target's view that yes, but your banks,

they acted in different ways. For instance, some of the banks immediately reissued cards. Some didn't do so immediately but, rather, contacted customers in the first instance before cards were reissued. All banks ultimately had to pay fraud charges. Anyway, the fact that banks had variations, if you will, of acting Target points to as saying, well, obviously, this is not a cohesive class. Your Honor, it's cohesive because banks were prompted and required to take action. What they did -- for instance, incurring costs associated with reissuance or incurring costs associated with fraud -- those are just various levels of damages, Your Honor. It doesn't mean that they didn't have to act, as Mr. Librock and as Dr. Cantor point out in their expert opinions, Your Honor. So banks had to take action.

Now we have a related argument from Target that says essentially, Your Honor, how can this be traceable to Target's malfeasance? Well, we've pointed out how Target had an ability but ignored that ability to act. They could have announced way back in November that they had been hacked, they chose not to, and that caused the 40 plus million cards to be compromised, Your Honor. But Target says, well, you cannot say that these costs are associated with what happened at Target. Well, wait a minute. We've defined our class, Your Honor, as those banks, those

financial institutions who received notification of the hack, the breach at Target. Now, that is information generated from Target that motivates and requires banks to take action and, as a consequence, it's directly traceable to Target.

Now, we've heard arguments like, well, somebody could have stolen Mrs. Smith's card simultaneous with the fact that it had been hacked, Your Honor. My suggestion, that would be the tail wagging the dog. All of the class members here received formal notification that the cards at issue had been hacked necessitating on their part action.

So what we have here is an economic impact -- that is, banks being faced with what at that time was the largest data breach in the nation's history, having to act. They did act in various ways. And we're asking, Your Honor, that the Court certify a class with respect to the two largest components of damage that occurred as a result of the hack. Those are fraud damages, Your Honor, and those are reissuance damages, Your Honor. We are positing those as the damages that can be determined in this case because our expert has determined that that type of damage can be determined globally on a group or collective basis. And she accounts for all kinds of things, like baseline fraud and cards being reissued already, and that type of thing, and she comes up with numbers, and those numbers are going to be

articulated in her expert report that is due next month, Your Honor. But, in any event, so we have damages. We can prove them formulaically. And Target says yes, but we have a right to assert various affirmative defenses, like comparative fault. The fault leading to this event, Your Honor, had nothing to do with the banks. It was a hack at Target. It had nothing to do with the banks.

Another argument that is made in the nature of an affirmative defense is, well, the banks failed to mitigate. Well, here they spend part of their brief telling us, well, we mitigated too much, we acted too much, we issued cards too fast, we paid fraud charges and we perhaps shouldn't have. Then in this argument they're saying, well, we didn't do that fast enough by mitigating quicker than they did.

Finally, they make the rather preposterous argument, Your Honor, that banks assume the risk of this type of thing and therefore they ought to be the ultimate stuckee. Your Honor, the business decision was made by Target during the 2013 Christmas season to not interrupt its holiday sales by either disclosing what had happened or erasing/scrubbing this malware off its system at that time. That's a choice they made. But the banks, Your Honor, who we represent should not be the stuckee, if you will, at this time to pay the cost, which amount to hundreds of millions of dollars, as a reaction to this hack.

Now, finally, Your Honor -- and I will reserve a minute or two or three, if I could to respond to whatever Mr. Meal says -- we find it entirely disingenuous for Target to stand before you and argue vociferously that this is not a case suitable for class treatment, it just cannot happen because, Your Honor, there are some multi-facetted reasons why the Court should not consider this as appropriately handled in a class context. At the very time, Your Honor, they are making that argument, and they have since last -- before April when we met in Florida been trying desperately to settle this case on a class-wide basis. All these concerns about differences between the banks that they are referring to and they responded in a different way, and some had fraud damages when they shouldn't have, and some should have reissued quicker, all those types of arguments apparently evaporate when Target wants to extrajudicially solve this matter on a class-wide basis.

Now, the Court --

THE COURT: Counsel, what you're saying is true, but, you know, you know and I know that settlements are kind of one thing and the formal determinations of class are a completely different thing. In this very case we have the consumer matter that's pending before the Court for a settlement on a class-wide basis. Nobody has stood up and went through the grounds here like we're doing this morning.

The same would be true in the other settlements that have occurred.

MR. CAMBRONNE: And we know because it's America, they can attempt to settle that way.

THE COURT: Sure.

MR. CAMBRONNE: But all these concerns, Your Honor, that they voice here about banks reacting differently and the like are concerns that really in the real world all I'm saying is don't make that much difference to Target. And I think that's an important overlay over all of the arguments, Your Honor.

I've got three minutes left and I'm going to sit down. If you would let me say a few words at the end, I'd appreciate it. Thank you.

THE COURT: Okay. Thank you very much.

Mr. Meal.

MR. MEAL: Good morning, Your Honor. Douglas Meal on behalf of Target.

I'm going to borrow your watch, Carl, so I can keep an eye on time. Do you mind?

MR. CAMBRONNE: I want you to.

MR. MEAL: Okay. Great. Thank you.

Like Mr. Cambronne, I'm going to jump right into the predominance issue, Your Honor. As you know, there's a bunch of other issues around class certification here, but I

do think that the briefs mostly focus on predominance so that's what I will focus in on in the time that I have.

Your Honor is aware of the fact that when you're talking predominance, the cases from the Supreme Court are very clear in terms of what the analysis needs to be. You don't presume compliance with 23(b)(3). You have to show actual conformance to the rule. That means that a party seeking class certification under (b)(3) has to prove, prove common issues predominate. That's *Wal-Mart*. And the proof that's required is the evidentiary proof that *Comcast* requires. These are Supreme Court cases that are directly relevant to the analysis, Your Honor, and set forth a very, very rigorous standard of proof and impose a duty of rigorous analysis, that's *Wal-Mart* again, in deciding whether or not that evidentiary proof is there. So here, in terms of analyzing predominance, the analysis needs to focus both on the liability issues and the damages issues to see whether common issues predominate.

In terms of a liability analysis -- now I'm talking about the *Halvorsen* case from the Eighth Circuit -- what *Halvorsen* says is the evidentiary proof required by *Comcast* must establish that a prima facie showing of liability can be proved by common evidence. So you need common evidence to establish liability in order to have the evidentiary proof that *Comcast* requires under (b)(3).

So when we talk liability here, we're not just talking issues of Target's conduct, but we're talking, for example, issues of injury and causation. Those have to be established via common proof under *Halvorsen*. And what *Halvorsen* says in regard to injury and causation, Your Honor -- this is the *Halvorsen* case, 718 F.3d at 78 -- is that in order for a class to be certified, each member of the class must have standing and show an injury in fact that is traceable to the defendant. And all of that has to be shown through common proof. That's what the cases teach.

So here -- and you heard Mr. Cambronne allude to this -- what plaintiffs are trying to do to satisfy *Halvorsen* in regard to injury and causation is say, well, two points: First of all, according to plaintiffs, every bank that had an account alerted on as a result of the Target incident did something in response to that alert. That's proposition one. So that's the causation piece -- or part of the causation piece: every bank that had an alerted-on card did something. And then the injury in fact piece, according to plaintiffs, is that anything a bank did in response, whatever it did, caused an injury in fact that's traceable to Target. So that's their theory of common proof. Everybody did something and anything somebody did caused an injury in fact. Those are the two legs of their theory under *Halvorsen* for meeting the common evidence

requirement.

So let's talk about the first piece: every bank did something. Well, what you heard Mr. Cambronne say just now is every bank had to do something under the FDIC reg that he alluded to. That's their whole theory of showing from an evidentiary point of view that every bank did something. He says essentially every bank had to do something; therefore, every bank did do something. That's the evidence. Their sole evidence that every bank did do something is that every bank supposedly had to do something. The problem with that theory is they just read the regulation wrong.

This is from, Your Honor, their own expert's report, paragraph 16. And you see in paragraph 16 what their own expert quotes the regulation as saying -- I'm reading from the middle of paragraph 16, Your Honor -- is "the Gramm-Leach-Bliley Act covered institutions must adhere to a response program designed to address incidents of unauthorized access to sensitive customer information" -- here's the important part, Your Honor -- "maintained by the financial institution or its service provider." This reg has zero application to a breach at a merchant like Target. You know how we know that, Your Honor? Not just because the lines in the reg make it clear that that's the case, but if you're a bank covered by Gramm-Leach-Bliley and this reg

kicks in, you are required to submit to the FDIC a suspicious activity report every single time this event occurs. Your Honor, guess how many suspicious activity reports were submitted by the named plaintiffs in this case to the FDIC resulting from the Target breach. Zero. Seven named plaintiffs. Zero suspicious activity reports. Why is that? Because every one of these banks knew this reg had no application to this situation. That's why those weren't submitted. And this whole idea that this reg somehow has something to do with this case is just something that was cooked up after the fact in an effort to get a class certified here.

Further indication that there is no such regulatory requirement, let's look at the best practices that Visa says are to exist in a situation where a breach like this occurs at a merchant like Target. Now I'm reading from Exhibit 48 to my declaration, Your Honor, the Meal declaration. This is Visa's best practices for dealing with an account compromise. And if you go into the best practices, you'll see the very third bullet under number one is the following. This is a best practice per Visa. "If you haven't seen any signs of fraud that you believe could be linked to the reported account compromised incident, continue to monitor your accounts in accordance with best practices," i.e. don't do anything different. That's what

Visa is saying. If the best practice is in many cases to do nothing, how can it be that the reg requires every bank to do something? Well, it doesn't require that.

And what did plaintiff's own service provider tell them to do here? This is Fiserv. This is Exhibit 7 to my declaration, Your Honor. What did Fiserv, their own service provider, tell them to do in regard to the Target case? Well, I'm reading from Exhibit 7 at the top of the page. This is the information when the alert is set out by Fiserv to its customers, these very banks. What did Fiserv say? "This information," meaning the alert -- the alert that, according to plaintiffs, is the clarion call that required everybody to wheel into action and do something -- "This information should be reviewed to determine what action, if any, is appropriate for your financial institution." Even Fiserv, their own service provider, is making clear you're not required, you're not expected to do anything. You don't necessarily have to do anything.

And so what actually happened here? What does the evidence show about what actually happened here? Well, first of all, here we are in 2015 and who here in this courtroom thinks that just because a bank is required to do something a bank always does what it's regulatorily required to do? Since when has that been something you just take judicial notice of? I would say you take judicial notice of

no way do we expect banks these days to do what they're regulatorily required to do. Doesn't 2008 teach us anything, that you can't just assume that? And what happened here? Well, first of all, again looking to Visa -- and this is, again, Visa FAQ. This is from our expert's declaration, Mr. Zalpuri, paragraph 44 at page 29. This is Visa's description of what banks do when a breach like this occurs. And I'm reading from page 6 of that. The question is asked and Visa says here's what issuers do: Issuers processes for responding to alerts -- this is the very alert that Mr. Cambronne was telling you about just now -- issuer processes to CAMS alerts very widely. "Some automatically reissue all or some of the account numbers listed. Some merely implement monitoring or enhance their current monitoring programs." Others use a combination of these approaches. Here's the punchline: Some "do nothing." That's what Visa says. That's the network that these folks are members of. Visa says some "do nothing." So when Mr. Cambronne stands up here and says everybody did something, that just isn't the evidence. And how do we know it's not the evidence? Because we actually took discovery of these very plaintiffs and we found out, yes, some did nothing. Some of these very plaintiffs did nothing.

Sterling Bank, which is now part of Umpqua, one of the named plaintiffs here, we took their deposition. It's

recounted at pages 7 and 8 of our brief. They did nothing. They just continued doing what they were doing. That's the testimony.

Then, Your Honor will remember that you authorized us to take some depositions of non-named plaintiffs. Remember that back a couple hearings ago? Well, we did that and we got declarations from two of them and deposed one of them. Pan Pacific, one of those entities, it acted. It did act. It reissued. Do you want to know when it reissued, Your Honor? Pan Pacific reissued when it got the subpoena in this case, the subpoena that we were going to use to prove that it did nothing. And in order to try and manufacture Article III standing and get the plaintiffs out of the box they were in by that, it reissued in response to our subpoena. That's not taking immediate action the way Mr. Cambronne was saying. It did nothing.

Home Federal, another one of those -- and that's discussed at page 49 of our brief, Your Honor. Page 55 of our brief discusses Home Federal, another absent class member that you gave us leave to take discovery from. Home Federal did nothing, absolutely nothing. It had a card. It did nothing.

So this proposition that everybody did something, the evidence -- and that's what Your Honor is under a duty to look at -- the evidence shows that in fact not every bank

did something.

Even if it were the case that every bank did something, which is not the case -- and which in and of itself defeats their whole theory of class certification -- even if that were the case, the second piece of their argument fails as well, and that's the proposition that just because you did something means you incurred an Article III injury in fact and that that injury is traceable to Target. That's the argument. There's no evidence of that. In fact, the evidence shows, again, the opposite.

Mr. Cambronne mentioned that they're focusing primarily on two categories of damage, Your Honor: fraud reimbursements and reissuance costs.

Fraud reimbursements. What does the evidence show about whether fraud reimbursements are traceable to Target in the way that is required under *Halvorsen*? What does the evidence show? Well, here is Umpqua Bank, the named plaintiff. We deposed Umpqua Bank. What did Umpqua Bank say? This is in our brief at page 31. Their own plaintiff said, "There is no way to know, no way to know whether the disputed transactions are connected to the Target breach." So they admit that the fraud isn't traceable to Target. There is no way to know if it's traceable to Target. What does the evidence show? The evidence shows that it's not traceable.

Mr. Cambronne mentioned the stolen card issue. That's Lorain Bank, another one of the named plaintiffs. This isn't just an isolated tail-wagging-the-dog situation, like Mr. Cambronne said. The "dog" here from Lorain Bank's point of view is that stolen card. The largest single fraud loss that Lorain incurred was on a stolen card. This is the actual plastic was stolen from somebody's wallet and a fraud charge was made. That's the bulk of Lorain Bank's claim. Well, that injury isn't traceable to Target. Target didn't steal that guy's card. That fraud has nothing to do with the breach. And that's the biggest claim that Lorain Bank, one of the plaintiffs in this case, is making.

Let's take CSE, another named plaintiff. CSE's entire claim in this case is based on PIN-enabled ATM charges where somebody got the PIN on a bunch of cards and made ATM charges. This isn't just the large part of their claim. This is the entire claim of one of the named plaintiffs in this case in terms of fraud losses. Well, there was no exposure of PINs in the Target breach. That's conceded. So any ATM-based fraud which was PIN enabled isn't possibly traceable to Target. So our discovery of CSE showed that they've got no claim in this case because they can't possibly trace their fraud to Target.

And in terms of reissuance is the other category, well, here there's actually -- this is the one point the

experts agree on. Both experts have submitted to you reports saying that just because you do a reissuance doesn't mean you incurred injury. That's the Cremieux report at paragraphs 40 to 43. And the reason for that, Your Honor, is obvious. Every payment card that I've got in my wallet, that you have in your wallet is going to be reissued sooner or later. So the fact that your card gets reissued sooner, rather than later, doesn't mean that the reissuer incurred an injury. In and of itself that doesn't prove anything with regard to injury. Mr. Cremieux, our expert, laid that out in detail in his report, that you can't assume injury just from reissuances, which is what the plaintiffs do. And then, in the supplemental report that plaintiffs submitted from their expert, Dr. Cantor, at paragraph 70 here's what she said: She said, "I agree that there are a number of scenarios for which the account reissuance would not be incremental or result in a material cost." So the experts agree, directly counter to what Mr. Cambronne just told you, the mere act of reissuance, if you did that in response to the breach, doesn't establish injury in fact. So that theory of proving injury and causation through common proof fails as well.

Quickly now, because I think -- where am I on time? About five minutes left?

THE COURT: Somewhere in there.

MR. MEAL: Bear with me a little bit, Your Honor, if you would, because I do want to talk about a couple of other issues just quickly.

First of all, in terms of the issue of the reasonableness or unreasonableness of a plaintiff's conduct here, that is squarely part of the liability analysis. We, through our discovery, established in the case of every single named plaintiff -- and it's all laid out it in our briefing, Your Honor -- that we have a substantial defense to every single plaintiff's claim based on that plaintiff's own contributory fault, whether it was Lorain Bank that just automatically knee jerked and reissued everything without doing any analysis (that's their own testimony) or the bank I mentioned before, Pan Pacific, that sat back and did nothing until it got a subpoena. There's tremendous, tremendous evidence to that effect.

Now, this is not just a damages issue, because under the Minnesota comparative fault statute, it avoids liability if the jury were to find that the plaintiff, as would be the case for example in Pan Pacific obviously, that the plaintiff was the primary -- at least 51 percent responsible in terms of the fault that led to the injury. So that would escape liability entirely. So this is not just a damages issue. But even if it were a damages issue, Your Honor, it still is a Seventh Amendment requirement that

in deciding comparative fault, whether it's for damages purposes or liability purposes, under the Seventh Amendment the same jury has to hear both sides of the fault story. So this can't be a situation where one jury comes in and hears the issue about Target's fault and then we have thousands and thousands of jury trials then deciding each individual plaintiff's fault. This is all got to be done at once because you can't have one jury decide -- the only way to decide the issue is the jury has to hear both and allocate fault appropriately.

So we cited the *TJX* case, which is dead on point on this. That in and of itself prevents class certification. You can't certify a class if you're going to violate someone's Seventh Amendment rights in doing so. That's fundamental.

What's also fundamental here -- I'm going to skip over a lot of the other stuff that I wanted to talk about because I know you've got limited time this morning, but --

THE COURT: We have some pretty thorough briefing here, too.

MR. MEAL: Yes. Understood. I do want to mention, though, a little bit on the damages issue, because this is something where their theory is running head long into *Comcast*, head long into *Wal-Mart*. And you don't even have to reach the issue of the reliability of Dr. Cantor and

whether or not Dr. Cantor has reliable methodology. We say she doesn't. We say when you weigh -- leaving aside the *Daubert* issue about whether her opinion is admissible, leaving that aside, when you weigh Dr. Cantor's analysis against Mr. Cremieux's analysis, our expert, and you do the weighing of the evidence that the cases require, we don't think there is a way to find that she's got a reliable methodology. But leaving that aside, Your Honor, there's two show-stopping roadblocks on their theory of class-wide damages, and the first is created by *Comcast* and the second is created by *Wal-Mart*.

Comcast says that to show class-wide damages for Rule 23(b)(3) purposes you've got to have that common methodology. And the first point on *Comcast* is the damages methodology has to be consistent with the liability theory. Their model fails that. Their liability theory, in terms of injury, you heard Mr. Cambronne explain it. Their liability theory is that everybody had some injury. They did something and that creates liability. That's the injury in fact for liability purposes. But their damages model doesn't purport to measure that injury. It doesn't line up. Their damages model, and Mr. Cambronne conceded this, only purports to address two components, two of the things that banks may or may not have done in response to the breach. Well, that's in direct violation of *Comcast*. They say in

their reply brief that *Comcast* doesn't say that, but in their reply brief they cite Your Honor to the *Roach* case. And I do want to point this out to Your Honor because it's very important. *Roach*, which they cite, is authoritative. Well, what does *Roach* say on this particular point? Here's what *Roach* says. I'm reading from the *Roach* case that they cite, 778 Fed.3d at 401, and this is, it looks like, page 407. "*Comcast* held that a model for determining class-wide damages relied upon to certify a class under Rule 23(b)(3) must actually measure damages that result from the class's asserted theory of injury." There has to be that link. That's what *Roach* says. *Roach* cites to the *Sears Roebuck* case out of the Seventh Circuit, which says the exact same thing. Their model doesn't do that. That's the end of the story. But if that weren't the end of the story, then you've got the *Wal-Mart* problem of their theory.

Wal-Mart holds that if you've got a damages model that creates what *Wal-Mart* calls "trial by formula," where you're relying on averages and then extrapolating those averages across the entire class -- and that's all what Cantor does in her report. It's average after average after average coupled with extrapolation after extrapolation after extrapolation; that's all she does, that's the whole thing. Well, *Wal-Mart* says you can't do that. That doesn't work, and it would violate due process. And absolutely you cannot

measure class-wide damages through averages. That's what *Wal-Mart* says. Now, in their reply -- we made that point in our brief.

In their reply they cite you to the *Air Cargo* case and says *Air Cargo*, which is a district court case out of the Southern District of New York, I believe, says that's not what *Wal-Mart* -- *Wal-Mart* doesn't hold that. When you read *Air Cargo*, Your Honor, you'll see it never even cites *Wal-Mart*.

The only case, the only case that has addressed this issue of the impact of *Wal-Mart* in terms of whether you can use averages the way Dr. Cantor proposes to use averages is the *Tyson* case, which, as Your Honor is probably aware, is up before the Supreme Court right now on this very issue. The argument is scheduled for November 10th. It's all fully briefed.

Now, in *Tyson* what the Eighth Circuit did is said, well, we think there might be an exception to the *Wal-Mart* prohibition on averaging when you're operating under the Fair Labor Standards Act. And here also there might be an exception when there is no way -- it's not just difficult, but there is actually no evidence that you could go to except accept an average -- and that's what the *Tyson* court said, sort of created an exception to *Wal-Mart*. And what the Supreme Court is considering now basically is whether to

recognize that exception. But in terms of the general rules, that exception has nothing to do with our case. This isn't an FLSA case. This isn't a situation where you can't get the information. We got the information. We did the discovery. We got the information. So this isn't that situation either. *Wal-Mart* blows out of the water their entire damages model.

So I appreciate your indulgence for a couple extra minutes. If you have any questions, Your Honor, I am happy to try and address them.

THE COURT: Okay. Thank you very much.

Mr. Cambronne, before you start with your rebuttal, to the best of my knowledge, the only data breach class case that's out there is Bill Young's decision. Why are you distinguished? He denied the cert -- or he denied the class. Why do you distinguish it?

MR. CAMBRONNE: Well, in that case, Your Honor, they did not have before the court expert testimony like we have, Your Honor, saying that the expert, and the Court therefore, has an ability to determine damages on a class-wide basis.

Our expert, Your Honor, meticulously is able to filter out, for instance, baseline fraud and baseline reissuance costs, and all that sort of thing and thereby attribute the losses that we are seeking here, Your Honor,

to the Target fraud. You will not find that in that case.

But furthermore, Your Honor, if we look at the common facts, Your Honor -- we have disagreements on some facts. For instance, we just heard Mr. Meal say that PIN information was not stolen during this matter. Target itself on December 27th, 2013 issued a press release and said, oops, we were wrong, PIN information was indeed stolen. Now, a jury can eventually make that determination, but it's a common fact, Your Honor. Either they did or they did not. As I say, this (indicating) is just a release from Target on that particular day that contradicts what Mr. Meal just said.

Your Honor, this is what we've tried to --

THE COURT: I can't get over this world I'm in today. Somebody wants to come up with rebuttal argument, they have the telephone.

MR. CAMBRONNE: Here's the proof, Your Honor.

In any event, we say banks had to do something and Mr. Meal says, yeah, but they didn't -- some banks acted quicker than others and references, for instance, the Sterling Bank and said, you know, they sat on it for a while. They had to pay huge fraud damages as a result of their inaction. That's the rest of the story with respect to Sterling Bank.

Target issues its own -- or did issue its own

called RedCard. They have the Target logo on them. Target reissued all of its cards, Your Honor, in response to the Target breach for those that were impacted at the time. Yet Mr. Meal will come up and say, well, we cannot assume that banks have to do anything. Mr. Librock points out not only the FDIC requirement, Your Honor, requirement of acting, but the other laws impact this and also a number of considerations that force banks to do something. Now, some banks didn't do it as quick as others, but they all had to do a heightened level of monitoring because they were told that these situations, and this situation, these cards have been compromised.

Mr. Meal would like you to conclude, Your Honor, that the FDIC guidance on unauthorized access to customer information really isn't anything, you should discount it. But it says in the very document that I alluded to and put up on the screen before, Your Honor, that financial institutions should provide notice to its customers whenever it becomes aware of an incident of unauthorized access to customer information. That's when an institution should provide information to its customer. Your Honor, they want to run from that requirement. They want to run from -- Target wants to run from the conclusions that Mr. Librock points out that we're bankers. We get notified of a breach. It's in the news. It's in every newspaper. And then we get

the CAMS alerts from Visa. Visa. Everybody in the world knows it. And there's a response of, well, maybe you should do something or maybe you shouldn't do something or you should do it faster or slower. That's, Your Honor, make weight in terms of the need to response because banks, like Sterling for instance, that chose to wait ultimately paid the price by enhanced fraud charges.

We have a situation here where banks are called upon by federal regulation to act under penalty, Your Honor, of having to pay enhanced fraud charges if they don't. And now Mr. Meal would like you to believe that, well, really some banks did it quicker, some banks did it slower. Your Honor, they're all impacted. That implicates the level of damages, not the fact that they're all implicated.

We've come forward, Your Honor, with information from an expert unlike that only other case. All the other cases, Your Honor, have really been resolved one way or the other, sometimes through the Visa mechanism where they settle cases outside the jurisdiction of the court. This is the only one -- the first one in the nation, Your Honor -- to my knowledge where a Court has been asked to certify a class based with sound expert testimony and, unlike that *TJX* case, I think it was called, and the fact that we've been able to develop common facts that lead to liability.

One more thing, Your Honor, and then I'm going to

sit down. You have also a unique situation facing you in that one of the theories of our case is the Plastic Card Security Act, which determines, Your Honor, as a matter of legislative policy that reissuance and payment of fraud charges are reasonable responses on the part of banks or financial institutions. And under that statute, Your Honor, merchant pays banks for the cost of those two items. That's a legislative overlay here that impacts what happens in this court because Target is subject to that statute.

To suggest that banks are all different out there and some move quicker than others, well, that's maybe true, but the fact of the matter is they all have to do something. If they get notified of a breach, they have to do something. Some choose to wait and see if there's any fall-out, like Sterling Bank. They did so to its peril. Others do it quickly, like Target itself replacing all their cards in response to this data breach.

The real world, Your Honor, is not these little anecdotes where Mr. Meal suggests, well, maybe possibly somebody's dog ate it and they ate a credit card. I know he didn't say that, Your Honor, but that's what he's suggesting. Your Honor, in the real world we have banks being notified, banks having to respond, and banks incurring damages, a classic and quintessential case, Your Honor, for class certification. Thanks.

THE COURT: Okay. Thank you very much.

Counsel, we thank you for the submission this morning and thank you for coming in. We'll take the matter under advisement. We'll try to let you know just as soon as we can.

As a factor I thought of just this morning candidly, and that's that at some point that we were together a couple months ago I said, well, after this motion is over we'll have a little status conference to find out where things are. I'll be candid, I didn't think about that until this morning that we, in fact, said it. And I haven't talked to Judge Keyes at all about any of this, but is there anything that's in the overall management that should come to my attention this morning? Mr. Zimmerman.

MS. ZIMMERMAN: Yeah, there is a small issue, Your Honor. We can take it up now or we can talk to Judge Keyes if you'd like --

THE COURT: Sure. Fire away.

MS. ZIMMERMAN: -- but it has to do with the completion of discovery.

Due to scheduling issues with certain witnesses, we have an agreement -- but we haven't agreed on everything -- to extend discovery to the end of October for the completion of discovery.

The disagreement we have is: Target's position is

we can go to the end of October for the completion of discovery that's already noticed, but we can't notice anything further to be completed by the end of October.

Our position is we should be able to also notice things that we need to notice. Primarily we need to know things about damages, things from American Express and third parties, the results of the Visa settlements, things like that that we perhaps haven't noticed yet but we will notice very shortly. And so we just don't want completion of discovery to be for things that have already been noticed, but to give us the opportunity to notice things. And we will do it promptly, in the next week or so, so that we can endeavor to complete it by the end of October.

Now, if there's a particular problem with a schedule or a witness, we can bring that before the Court or have the indulgence of counsel, but the general understanding we think should apply is we'll complete it by the end of October, but we're not limited to things that have already been noticed.

I think Michelle or Doug may comment.

MR. MEAL: I'd like to address that, Your Honor.

THE COURT: Sure. Mr. Meal.

MR. MEAL: So like we've done throughout, we're trying to be cooperative here, we really are.

THE COURT: Sure. Well, frankly, I commend all of

you on this overall subject. You folks have done, I think, an outstanding job of keeping away from me. That's good.

MR. MEAL: And so we've tried to do that, and we want to be cooperative here, but there does need to be an end to this. I mean, this scheduling problem that Mr. Zimmerman alluded to is created by the fact that over the last, I would say, three weeks they have all of a sudden launched a blizzard of deposition notices. The plain fact of it is, unless we went to a quintuple track, we couldn't complete what they've already noticed by the end of September.

Now, Your Honor's scheduling order says that the deadline is October 1, and all discovery has to be noticed so it can be completed by October 1. That was the deal. We could've taken the position that all these depositions you're now launching are inconsistent with the deal, because there is no physical way to get those depositions you are now noticing done by October 1. It cannot be done. I mean, we're three weeks away at this point. So we didn't say that. We said we don't want to be jerks about this, we want to be fair, and we know you're in a position where you want to take discovery that you can't get done by October 1, and we'll accommodate that and move it out so we can let you complete what you've noticed. But this isn't going to be opening the door that now that you've got until whatever we

agree to -- at one point October 15 was on the table, then the end of October was on the table. This isn't going to be a situation where now we've opened the door and now other discovery gets to be noticed that clearly would've been barred at this point under the order.

We do think we've been extremely cooperative. We've spent incredible effort on doing fact discovery in this case. And we do think that the time has come to call it a day in terms of noticing yet more discovery. And we don't think our agreement to be accommodating should be held against us and be a vehicle for doing that.

So I wasn't really imagining we were going to be arguing this particular issue before Your Honor this morning, but I do want to stress two things: First of all, we are absolutely trying to be cooperative, and the offer we made was an effort to do that. But at the same time, I think with all the discovery we've given, tons of depositions, at some point it needs to end. We think now is the time it should end in terms of nothing further gets noticed. So that's our thinking on it.

THE COURT: Okay. Thank you very much.

Anything further?

MS. ZIMMERMAN: No, Your Honor. I'd just be repeating myself.

THE COURT: Okay. Counsel, it strikes me that,

number one, I'll start with this, and that's simply to say that I'm the first to admit that the scheduling order that we entered in this to start with is a very aggressive order. And I say that because it's something I believe in. I believe in moving litigation through the process as quickly as possible on one side of the coin. On the second side of the coin, I also believe that everybody that's involved in this piece of litigation is in business. And if there's anything in this world that a business person doesn't like is uncertainty. They want decisions. And, frankly, that's why encouragement of a very aggressive schedule was developed on it.

Having said that, number one, I'm going to permit the extension of the cut-off of the discovery to the 1st of November, staying with I have a predilection to do everything on the first of the month.

Secondly, I am going to authorize the additional noticing that was discussed. And if any aspect of that additional noticing is unfair, I would encourage that it be brought to the magistrate's attention on an expedited basis and let that be discussed individually as to what particular discovery might be that's requested. Okay.

MR. CAMBRONNE: Thank you, Your Honor.

THE COURT: Thanks for coming in today. We'll let you know on this just as soon as we can.

MR. MEAL: Thank you, Your Honor.

(Court adjourned at 10:58 a.m.)

* * *

I, Debra Beauvais, certify that the foregoing is a correct transcript from the record of proceedings in the above-entitled matter.

Certified by: s/Debra Beauvais
Debra Beauvais, RPR-CRR