2007, your testimony is that Mr. Maslowski's authorization to initiate wire transfers had been revoked by Experi-Metal, is that your testimony?

A Yes.

Q How did Experi-Metal revoke his authority?

A By signing an agreement with Valiena and Experi-Metal to basically say that she and Gerald were the only signers on the wire transfer and that he was basically off and had no access to any of this. It was through a couple of agreements that are in exhibits.

Q But he's not mentioned on that document at all, is he, his name isn't on that document?

A The name actually would be that these are the only two people that are allowed to wire transfer from this company's account.

Q Shouldn't there have been a revocation of his authority in writing?

A That would be the responsibility of Comerica to decide, not me.

Q Have you ever seen a form like that before you saw it in this case?

MR. TOMLINSON: A form like what?

MR. HOLLEMAN: The form that he's relying on, the December 1, 2007, document that he just referred to.

THE WITNESS: Can you pull that out? I don't want

EXHIBIT 1c

to comment on it until I'm looking at it.
BY MR. HOLLEMAN:
Q Sure. Plaintiff's Deposition Exhibit 5, I think.
A Okay. So the agreement here basically decides who are the initiators for wire transfers. This one says not applicable. That person is not an initiator. So by rules at 1 and 2, we're saying Valiena and Gerald have access to wire transfers and no one else, and that's how that is understood in this contract. From me, as a non-lawyer.
Q And have you ever seen a form like that before you were shown one in the context of this litigation?
A I have seen a form similar to this for my own personal bank account, my own business bank account.
Q But never in the context of evaluating a bank's performance to industry standards, is that right?
A No, I have not seen that, no.
Q Is it your understanding that this document has to do with the calling in of wire transfers versus online wire transfers?
A That is my understanding, yes.
Q Within the TM Connect web application, do you know if -- wasn't Ms. Allison the administrator within the TM Connect web application for Experi-Metal?
A From what I understand and I've read, yes.

Q So she had the authority to designate who within the TM Connect web application could initiate wire transfers and who could not, right?
A According to what I've read in Comerica's policy, yes, she has that authority.
Q And isn't it a common feature in web-based commercial banking applications that a customer is the person who determines who has access to certain applications or who can take certain actions?
A When you say customer, you mean the business customer, as in Valiena being the administrator and that customer, connecting all the question together?
Q Yes.
A Yes, then that would be somewhat common, yes.
Q Do you know if Ms. Allison checked Mr. Maslowski's authorizations when she received his token in 2008?
A In 2008, if she checked like as in contractually checked, did she check online?
Q Did she check his online authorizations or rights within the TM Connect web system when she received his token?
A I would -- the answer technically is I don't know if she did. Or if they were even available to check.
Q Did you interview Ms. Allison in preparation -- in preparing your report?
A No, I did not.

Q Did you interview Mr. Maslowski?
A I did not.
Q Did you talk to anybody at Experi-Metal?
A I have not talked to anybody at Experi-Metal, no.
Q Is Comerica in your opinion -- well, let's look at your opinion number 3 on page 9. With respect to your opinion number 3, do good faith and industry standards require that Comerica notify its customers every time that it becomes aware of a phishing scam or e-mail?
A I would say that it is the proper response when dealing with phishing attacks, yes, and it is the common method by the majority of banks.
Q What if it's reported by a non-customer?
A So a non-customer? It also would be common -- if it's reported by a non-customer, like say I reported a phishing attack to, say, Comerica, it gets reported to their abuse department and then gets escalated and then it should be still notifying their customers because it is a publicly available event.
Q What if it's directed only to non-customers so that the bank doesn't know about it?
A The bank can't control whether they know if it's non-customers or customers.
Q What if it's only directed to ten customers, does the bank have an obligation to report to all customers --

A The bank --
Q -- this threat?
A Yes, because you can't -- okay. So I'm going to process this here for a second so that you'll understand the way phishing works. When a mass e-mail gets out, it doesn't get sent out to ten people in most cases at all, I don't think I've ever seen one like that, that's not targeted, and what's the point of targeting non-customers of Comerica? So when they send out a mass mailing, there's at least a list of between 100,000 and 10 million e-mail attempts on that list in hopes that there's some banking customers at Comerica. Some of these attackers will actually figure out who is a customer and start tailoring those lists better and making better targets.

The problem with it is that any bank will not usually know how many mass mailings were sent out because it's in people's inboxes and for violation of any privacy we can't, obviously, tell how many e-mails went out to how many people, so their obligation is to realize that it's a high risk when that happens and that they have to assume a worst case scenario, that even if one customer gets compromised, they need to make best efforts to protect all their customers, and phishing attacks are designed to get as many of their customers' information as possible.

Q Phishing e-mails are a form of spam, right?
A They are a form of spam.
Q And there's a huge volume of spam that goes out every day, right?
A There is.
Q There's a huge volume of phishing e-mails that go out every day, is that correct?
A There's a good size, yes.
Q So did Comerica need to alert customers every time a phishing e-mail went out when the volume is like a spam?
A It's not that common against Comerica. And the ones that do get common ones keep that warning up.
Q What is the duty -- I'm sorry, what is the -- what does good faith and industry standard require Comerica's notice to say?
A The notice is basically to alert the customer that there is a fraudulent attack against the Comerica users and to not click on links and do not take -- leave in any e-mails that basically request your user name or password. Basically, and if you have questions, please give us a call, like if you're not certain if you're at our real site. Basically, the idea of the e-mail is to educate the user so that they obviously are in host.

Also, if the user feels like they were a victim, they are asked to call the bank to report it, and if

they -- if they're not certain, they're still asked to call the bank and basically make sure that their account is safe. Basically, they're trying to -- the idea is it's an alert, and that alert comes with education.

Q How soon must the notice go out after the bank becomes aware of the phishing e-mail?

A As soon as possible.

Q So it can vary depending on the circumstances?

A Well, if they're aware of it, which it's their job to be aware of it, then they should send it within probably like an hour, at least, because it takes -- the first ten hours, the phisher gets most of the accounts that they need.

Q So your good faith standard would be one hour within receiving notice of a phishing attack that it go out?

A I would say as soon as possible is really what is occurring. And once you observe or are aware of it, whether a customer let's you know, whether you have a spam trap that sees the attacks, whether someone in the industry let's you know, hey, there's a phishing attack going out, especially one that is very specific to 2009. That one was a very specific style of attack and it held high -- a high amount of threat due to the fact that it was targeting not only business customers, but it was also targeting the way that -- it knew their internal

systems, they knew those systems.
Q In your view, is Comerica ever entitled to rely on a previous notice given and then the customer's obligation to be aware of that notice and not provide its information in response to a phishing e-mail?
A No. And in my view, that is -- that would not make sense.
Q So your --
A I think it's very specific and most of the e-mails should be specific.
Q So your testimony or your opinion is that every time there's a new phishing e-mail targeting a bank, the bank should send a specific notice to all of its customers related to that phishing --
A Or invent technology that allows them to be alerted when that goes on, yes.
Q Has phishing decreased since 2009?
A When we define phishing, if you're talking about specifically phishing with the attempt to just steal credentials from another web site, that method has decreased because malicious software has increased, but they use phishing techniques to deliver the malicious software. So the activity of cybercrime has not really decreased, but the activity of specifically phishing via e-mail, faking a bank account and all that stuff, has

specifically decreased because of the substituted next evolution.

Q So the tactics of the criminals or fraudsters have changed?

A They have changed. Where they've more applied -- they've been kind of the same for a while, but they now are going, hey, this works better. So yes.

Q If you look at page 9 of your report, still under paragraph three, but the -- under number 3, but the one, two, third paragraph under your numbered paragraph, one, two, three, it says "Industry standards have developed," do you see where I've started there?

A Yes.

Q Whose standard -- you say industry standard, but where does the industry standard come from whereby banks quickly notify their customers of the imminent threat of known phishing e-mails and potential phishing attacks directed to the bank's customers?

A If we pull up even, I think, FFIEC, it comes under alerts and responses. There's multiple different -- other than -- I can even -- other than FFIEC, FS-ISAC, which is a banking committee, has agreed that that is the appropriate response. Also, the Anti-Phishing Working Group has agreed that that is the appropriate response. The Digital PhishNet, which is a

Microsoft-sponsored consortium, has also decided that's the most appropriate response. The NCFTA, which is the National Cybercrime Training and Forensics Alliance, which is an FBI organization, has decided that's the responsible -- the response. The Secret Service, it's on their web site. The FBI, it's on their web site. So there are multiple places that you can sit there and define that this is good standard, good practice.

Q Is there one particular way that is required by these --

A Of course --

Q -- by these industry standards to notify customers?

A We were discussing industry standards. Not all industry standards, like we said, including -- they're mostly guidelines and nothing is required, it's in general, most of these things cannot be required of any -- an institution due to -- so there's no requirements respective of this -- this is not a requirement, no.

Q How many times does something have to occur for it to become an industry standard?

A I guess that depends on the situation and what is the occurrence.

Q Do you know if Comerica took any steps to warn its customers on January 21 and 22 of the phishing attack, 21 and 22 of 2009 of the phishing attack?

A I was not aware of any steps to specifically address

that phishing attack in the sense of warning its customers, no.

Q In your opinion, was Comerica entitled to rely on Mr. Maslowski at all to safeguard Experi-Metal's log-on I.D., password, and token information?

A Let me just repeat that so I'm very clear.

MR. HOLLEMAN: Go ahead, or she can repeat it.

(Record repeated.)

A Do I believe Comerica is responsible is the question? Or --

BY MR. HOLLEMAN:

Q No. I asked the question --

A The last part of it, please.

(Record repeated.)

A In my opinion, I believe that through possible like education with -- you know, of the customers, you increase the reliability, but in my opinion, I think that most of the actual safeguard should be implemented and taken care of mostly not by Keith, but actually on the banking end.

BY MR. HOLLEMAN:

Q So could Comerica -- was Comerica entitled to rely in any way on Mr. Maslowski safeguarding his information, yes or no?

A No, they must assume that the system is already

compromised.
Q Look back at Exhibit Number 30, which is excerpts from your book.
A Sure.
Q And if you turn to page six of the exhibit, but it says page 80 down in the bottom right-hand corner.
A When you count six, you're counting from page six, correct?
Q Page one. That page.
A Okay, thank you.
Q Do you see the shaded portion of text on that page?
A Um-hmm.
Q Is that something that you drafted or is that something that you pulled in from somewhere else?
A Let me read it real quick. Well, the Moore law, obviously, is what I pulled from Webopedia, I've obviously cited, and the actual text itself of the prior stuff is what I drafted, yes.
Q So you wrote "The most expensive security tools and firewalls cannot stop such simply conceived attack vectors because at the heart of every security problem, there is a human," end quote?
A Yes, and the context of that is actually very specific.
Q Are you saying that that doesn't apply to -- generally to information security problems?

A No.
Q So that only applies to a specific information security problem that you're referring to in that --
A Yes, this --
Q -- paragraph?
A -- is specific to certain types of phishing attacks, and we're talking at the level of just the authentication piece of tricking the user, where there's, again, there's defense in depth. This, we're talking about here's these fake sites and it can trick a human. And that's a fact, we're not denying that. And so what I'm basically covering is these are basically focused on social engineering can definitely trick a human into falling for something, but that's why we have more than one tool out there for the rest of it. If you're -- if you do fail at authentication, then you have X and you have X and you have X to protect you, don't rely on just a steel door when a window might be wide open.
Q But at the heart of responding to a phishing attack and that security problem, there is a human there, right?
A Yes.
Q So your statement as it's said on page 80 of your book applies to phishing attacks too, doesn't it?
A Yes.
Q And then you would agree with me that the weakest chain

in banking security is the customer, wouldn't you?
A That is true.
Q With respect to your opinion number 4, are you aware that there is an agreement between Comerica and Experi-Metal that allows there to be overdrafts on Experi-Metal's accounts?
A I am -- I don't think I'm officially aware of their overdraft agreement.
MR. HOLLEMAN: This has already been labeled Deposition Exhibit Number 39 in plaintiff's books, but I just have copies here that I will provide you.
MR. TOMLINSON: What are we going to label it?
MR. HOLLEMAN: It's already your Deposition Exhibit 39, so -- unless you want me to mark it again, I can.
MR. TOMLINSON: So this is -- this is Exhibit 39 and it relates to changes to the deposit accounts?
MR. HOLLEMAN: This is your Exhibit 39. I'm not going to agree with your characterization.
BY MR. HOLLEMAN:
Q I've handed to you Plaintiff's Deposition Exhibit Number 39 and I just want to ask you, have you ever seen this document before?
A Just give me a second.
Q Sure.

MR. TOMLINSON: Take your time and review it.
BY MR. HOLLEMAN:
Q Yeah, absolutely.
A This is very hard to see.
MR. TOMLINSON: I think he's just asking if you've ever seen the document.
A There's a lot of documents that were presented, so this one I specifically do not -- I'm not familiar with.
BY MR. HOLLEMAN:
Q Okay. I'm going to hand to you what's previously been labeled Defendant's Deposition Exhibit Number 11.
Have you ever seen that document before?
A No.
Q So if there are agreements between Comerica and Experi-Metal that allow there to be overdrafts in Experi-Metal accounts, then your opinion on this issue would have to change, wouldn't it?
A It would have to change if it's occurring to a savings account.
Q Where does your opinion refer to a savings account, anywhere?
A I don't know if I necessarily noted a savings account, but if the overdraft is in a savings account, then that's why my opinion may not change right away, unless there's specific evidence showing that the savings

accounts even have overdraft protection.
Q So your statement is that if there are agreements that allow overdrafts in savings accounts, then your opinion would change?
A If -- two things. If Comerica offered savings accounts with overdraft protection and provided that, I'd have to possibly look at that as an issue. But I would not change my opinion due to the amount that was actually overdrafted over. The activity involved in this would be still unusual for Experi-Metal -- anybody at Experi-Metal to be doing. Transferring over $50,000 in a zero size bank -- balance account is -- we can almost prove historically it's probably never been done by Experi-Metal.
Q But your opinion number 4 in your report relies on terms of written agreements, right?
A Correct. But -- okay.
Q When you refer to a, quote, unquote, sweep account, do you have -- did you learn from anyone how Experi-Metal used its, quote, unquote, sweep account?
A I'm not privy to all of the understandings of how they used their sweep account. In general, I don't -- my expertise wasn't required for understanding their business practices.
Q And you didn't review their business practices, did you?

A It is not my -- I didn't feel it was part of -- needed in what I'm looking at.
Q So when you're referring in your opinion to a sweep account, you're applying some general definition you have of what a sweep account is, isn't that right?
A I'm applying it to what the definition was actually held by based on the analysis of what I was looking at, it was called a sweep account, and I'm referring to the sweep account.
Q Who called it a sweep account?
A Both -- the documents that I had from Comerica is basically what was calling it a sweep account.
Q Ms. Allison could have named it a sweep account, right?
A That's true.
Q And it wouldn't -- that's fine.

Page 10, about the middle of the paragraph under your opinion number 6 -- I'm sorry, that's not right. Right under your paragraph 5, the sentence that starts "The documents in this case," do you see that?
A Um-hmm.
Q And it ends with "failed to respond to and report the information in a timely fashion," do you see that?
A Yes, I see that.
Q Okay. In your opinion, what would have been a timely fashion?

A In my opinion, this opinion is based on the specific events, not overall banking events. Again, these are all dependent on, per se, say we have monitoring in place, okay, like say you have some kind of system that can see this all the time. My opinion is based on -- a timely fashion for this, I think she should have been notified within two minutes.
Q How much time have other banks taken to respond to similar types of notifications?
A Almost immediately, between two to five minutes.
Q How do you know that?
A Because I've experienced it personally and I've also assisted with them on identifying other fraudulent activity to assist in getting them to get to a response.
Q How many times?
A I can't count it, I don't recall, but it's multiple times, we handled fraud for a lot of banks.
Q More than ten times?
A Yes.
Q What is the industry standard?
A What is the industry standard?
Q For how long it should take to respond to and report the information?
A Industry standard is based around the components that should be involved, and those components should

basically provide you a timely fashion. That timely fashion, again, is based on the individual events, the history of the person's records. In this specific case, the industry standard notification should have been between two to five minutes.

Q Should the bank take any time to verify with the customer that the activity is not in fact authorized?

A Very much so.

Q Might that take more than two minutes?

A She should have received a call within two minutes of the transfer starting to initiate.

Q Should there be any time internally to verify that access to the account should be blocked?

A Internally, one of the first requests was --

THE WITNESS: Can I pull out 456 real quick?

MR. TOMLINSON: Um-hmm.

A I just want to make sure I'm quoting correctly. The first request was for $25,000. She hasn't used probably wire transfer since 2007. Within, I don't know, a minute, there's another one for the amount of $250,000. Within another minute, we have 27,340. My point is, is that they have had -- immediately, one, there should have been automated systems in place that go, wait, there's something weird, please check this out internally and call your customer within two minutes.

BY MR. HOLLEMAN:
Q So your testimony is that as of two minutes after that wire transfer going out, Comerica should have called someone at Experi-Metal?
A Of being initiated, yes.
Q And your testimony is that that is what the industry standard compels?
A It does compel this, yes.
Q What is the purpose of a Fed or SWIFT message being sent to a bank?
A Usually it's for routing perspectives and to make sure that it goes offshore. SWIFTs are usually basically a destination point, so if it's going to, say, Hong Kong, you have a SWIFT route for that.
Q But every Fed or SWIFT message received by a bank doesn't indicate that there's fraud, right?
A No, not all the time.
Q In your view, does making a mistake equal not acting in good faith?
A Mistakes are one thing. In my view, making a mistake is not always -- one mistake is not always acting in -- is not saying it's a bad faith. It's a mistake. Mistakes can happen. Again, quoting my book, we are human.
Q In your opinion, is a mistake -- does a mistake equal not acting in accordance with reasonable commercial

standards of fair dealing?
A I can't answer that. My job was industry standard, my --.
Q Okay. Here you would agree with me that Ms. Jernigan made a mistake, wouldn't you?
A Yes.
Q Did she in your view exhibit bad faith in making that mistake?
A She exhibited negligence, yes.
Q Is negligence equal to bad --
A To bad faith, yes, I believe that she actually -- this wasn't -- the way I look at it, these type of mistakes are -- they deserve consequences because this is careless, this isn't mistakes, this is motivated by -- you know, it's not -- it's obvious, like how could you make mistakes? If you've been to the bank, you should know these policies, you should do this. They somehow have acted like they've never responded to one before.
Q So just so I'm clear, your testimony is that negligence equals a lack of --
A My testimony is that -- sorry.
Q -- negligence equals a lack of good faith?
MR. TOMLINSON: Objection, you mischaracterized what he just testified to.

A Negligence is a portion of a lack -- it is a component within the lack of good faith.

BY MR. HOLLEMAN:

Q Okay. What else is a component of a lack of good faith then?

A They lacked best efforts, they didn't make -- you can say she committed one mistake, but there's multiple mistakes that have occurred to pretty much end up in seven hours of losing -- constant wire transfers being sent out.

Q So the components you are testifying to that make up a lack of good faith are negligence and a lack of best efforts?

A And not following industry standards.

Q And not following industry standards. Those are the three elements?

A For me, for what I'm basing my report on, I'm looking at could this have been prevented by actually following -- making your best effort, following industry standard, and being not careless and focusing on -- I mean, a lot of it was a care -- there was carelessness involved and there was no organization of policy or any kind of thing that was -- you can tell by the way it was done there was nothing dictating any kind of standard to handle this problem.

Q In your view, does there have to be any intentional wrongdoing to equal a lack of good faith?

MR. TOMLINSON: Object to the extent it calls for a legal conclusion, but you can go ahead if you --

A I'm not going to -- I will -- I'm not going to answer that until I have further clarification. Not from you, but just in general, I would have -- I'm not at this time able to answer that.

BY MR. HOLLEMAN:

Q Your testimony to the United States House of Representatives consisted of you submitting something in writing, right?

A Yes.

Q You didn't testify in person?

A I did.

Q You did?

A Yes.

Q And that was -- and you submitted something in writing?

A Yes.

Q And that wasn't -- that didn't have anything to do with phishing, did it?

A It was mostly focused on telecommunications, but involved many of the main acts and the same actors as phishing, but it directly did not have a phishing pretense to it, no.

Q It didn't mention phishing at all, did it?
A It did, actually, it did mention social engineering, pretexting, and phishing concepts with Caller I.D., yes.
Q And your report indicates that you're being paid $350 for your testimony in this -- $350 an hour for your testimony in this case, is that right?
A Yes.
Q And Experi-Metal is paying that?
A Yes.
Q I just want to quickly go back to one area we had talked about before, and that's the entities that you had listed off that you've done work or provided technical advice to, the financial institutions.

Do you have a contact person that you worked with at PNC Bank?
A Samuel Strohm.
Q Do you have a contact person you worked with at Wells Fargo?
A Om Dixon.
Q I'm sorry?
A Om, O-m, D-i-x-o-n.
Q Do you have a contact person you worked with at TD Waterhouse?
A He no longer works there, but his name was Robert -- I'm trying to remember his last name, but also Bill Edwards

when TD Ameritrade came in was my last contact there, so Bill Edwards.

Q What about at Citigroup?

A Yes, Vishant Patel.

Q Could you help us with that first --

A I'm sorry. V-i-s-h-a-n-t P-a-t-e-l.

Q What about at Charles Schwab?

A I'll have to pull up the name. He may or may not be there and I don't remember at this time.

Q What about at Wachovia?

A It would be through OM Dixon, the same.

Q So you worked for Wachovia first, and then when they merged with Wells Fargo --

A I worked for Wells Fargo first and then also extended to Wachovia.

Q Who at Chase, anyone?

A I don't believe I mentioned --

Q Oh, it's just listed in your report.

A Okay.

Q But there's nobody in particular you worked with at Chase? Because I don't think you had a contract with Chase --

A Yeah, I didn't have a contract with Chase. Thank you.

Q Is there anything in addition to or different from your report that you plan on testifying to at trial in this

case?
A I believe at this time there is nothing unless, obviously, new discovery comes in or something, but other than that, no, at this time I'm happy with the report.
Q Is everything that you reviewed listed in the report?
A Yes.
Q Have you drafted anything other than your report that you plan on using at trial?
A No.
Q Have you consulted with any other individuals other than Mr. Tomlinson with regard to forming your opinion?
A No.
Q I just want to quickly look back at Exhibit 30.
A Is that the book again?
Q That's the book, yes.
MR. TOMLINSON: It's up here.
BY MR. HOLLEMAN:
Q And I want you to just tell me -- look through each page that I've attached as Exhibit 30 and just authenticate for me or tell me that these are indeed pages from your book?
A Yes, those are all pages to the book.
MR. HOLLEMAN: Okay. Thank you, Mr. James.
MR. TOMLINSON: No questions.

(Discussion held off the record.)

MR. HOLLEMAN: Back on the record. We've stipulated to the fact that Exhibit 3 to Mr. James' report is to be treated as confidential under the terms of the parties' and the Court's entered protective order.

(Deposition concluded at 12:39 p.m.)

* * *

State of Michigan)
County of Oakland)

Certificate of Notary Public - Court Reporter

I certify that this transcript is a complete, true, and correct record of the testimony of the witness held in this case.

I also certify that prior to taking this deposition, the witness was duly sworn or affirmed to tell the truth.

I further certify that I am not a relative or an employee of or an attorney for a party; and that I am not financially interested, directly or indirectly, in the matter.

I hereby set my hand this 15th day of January, 2011.

Elizabeth G. LaBarge, CSR-4467
Certified Shorthand Reporter
Notary Public, Wayne County, Michigan