THE CONSUMER FINANCE PODCAST: *WIRE FRAUD SCAMS – WHAT YOU NEED TO KNOW*
HOST: CHRIS WILLIS
GUESTS: SUSAN FLINT AND MARY ZINSNER
POSTED: OCTOBER 20, 2022

Chris Willis:

Welcome to *The Consumer Finance Podcast*. I'm Chris Willis, the co-leader of Troutman Pepper's Consumer Financial Services regulatory practice, and I'd like to welcome you to our podcast episode today, which is all about wire fraud scams and who bears the risk of loss. But before we get into that topic, let me remind you to visit and subscribe to our blog, consumerfinancialserviceslawmonitor.com, where you'll find daily updates about everything going on in the consumer finance industry. And don't forget to check out our other podcasts, we have three of them. We have our credit reporting one called *FCRA Focus*, our crypto-related one, *The Crypto Exchange*, and our privacy and data security podcast, called *Unauthorized Access*, all of which are available on all the popular podcast platforms. And if you like this podcast, let us know. Leave us a review on your podcast platform of choice.

Now, as I said, today we're going to be talking about wire fraud, and wire fraud cases arising from business email compromise continue to proliferate. The FBI has reported that from 2014 to 2019 business email compromise and other internet-enabled theft, fraud, and exploitation resulted in actual financial losses of $2.1 billion. And it doesn't just affect individual consumers. Even sophisticated parties and publicly traded companies are getting caught in these scams.

When this type of scheme happens, once the money's wired from one account to another, it's typically not recovered, and tracing the funds can become very difficult. Typically, litigation ensues, and the question arises of who bears liability in these cases and what claims can be asserted. These questions arise regularly in wire fraud cases, which our group handles a lot, and they often involve very large numbers and the imposition of loss on unsuspecting parties. Now, that is a big problem for the financial services industry and depository banks in particular, and I have two of my partners who are the perfect ones to tell you all about this on the podcast today. So let me welcome both Mary Zinsner and Susan Flint, two of the partners in our Consumer Financial Services group. So, Susan, Mary, thank you very much for being on the podcast today.

Susan Flint:

Hey, it's terrific to be here, Chris. Thanks.

Mary Zinsner:

Chris, thanks for inviting me. This is a topic I have a lot of interest in, so really appreciate the chance to talk about it.

Chris Willis:

Well, a lot of interest is on my part and on the part of our audience, too. And because the two of you are so experienced in these types of cases, I'm really looking forward to having you share your insights with the audience.

So, Susan let me start with you. Can you tell us about some typical wire fraud schemes that you've seen in cases you've handled for bank clients?

Susan Flint:

As you mentioned at the start of the podcast, there's a typical business email compromise situation with wire fraud, and it's otherwise known as the BEC fraud. So, you could look that up as well online and get some statistics around business email compromise. But the fraudster basically is someone who's trying to get access to someone else's money, and he impersonates either a trusted partner in maybe a company situation or in even a consumer situation, might impersonate the title company or a realtor or someone who has a relationship already with that consumer or customer. And that customer will often be duped by that fraudster gaining access to the details of the financial transaction, and they often will do that through the hack of one of the party's emails, and it could be any of the parties involved in the transaction might have a security breach somehow, and that gives the fraudster the information they need to pursue their fraud and their scam.

And so, essentially what they do is they'll reach out to that trusted partner or that victim customer, and they will change the account number on instructions that have already been given to the trusted partner or that victim customer. And they'll provide new wiring instructions in order to pay a debt or to conduct a real estate closing. And the real estate closings are really extremely common areas where we're seeing a lot of email compromised fraud. Or fulfill a purchase order, pay off a vendor. They'll change some information that allows that money to be basically rerouted into the fraudster.

So, the recipient of that email or that information from the fraudster does not notice that there might be a very subtle difference in an email address for example. It might have originally been from johndoe@abctitle.com, but in fact, the fraudster puts an underscore in the middle of the email address, which you may or may not notice, and it becomes johndoe@abc_title.com. And so, if you are the victim, you're not going to notice necessarily that there's a hyphen or an underscore in the email, and you're going to think it's legitimate. So, you will comply with that request, believing that the person you got it from is, in fact, a trusted partner and this is in fact what you're supposed to do.

You will then direct your money to be wired by the originating bank, that's the bank who initiates the wire at your request, to the fraudster's account, which is at the beneficiary bank. And the beneficiary bank is what we call the bank that receives those transferred funds. The beneficiary bank will generally have no idea its customer is a fraudster. And so, it is the ordinary course of business that transaction will go through. The fraudster, of course, is watching this very carefully and will immediately withdraw the money or transfer the funds before that fraud is detected, and it successfully pulls off, then, their fraud, their scam. And there's very little that either the sender or the banks involved in the transaction can do to claw back those funds.

Chris Willis:

Susan, thanks for that description. And particularly since you mentioned that it frequently arises in the context of real estate closings, it sounds like these scams can involve very large sums of money. So, Mary, when that happens are either of the banks that are involved in either initiating or receiving the wire transfer on the hook for those losses?

Mary Zinsner:

That's a great question, Chris, and usually it's what most people think, that the banks are liable, and it's why we see a lot of these cases. But the circumstances where banks can be held liable are very limited. So, the lawyers for the parties who are victims of wire fraud frequently file

lawsuits against the financial institutions involved attempting to craft claims alleging various common law claims such as negligence, and they try and allege negligence outside of the wire transaction itself to avoid some of the preemption principles that I'm going to talk about. So, for example, we see a lot of complaints that allege that the beneficiary bank, the bank that received the funds that were wired, was negligent in opening the account of the fraudster or failed to know its customer or failed to take prompt action to stop the withdrawals from the account once they were on notice of the fraud.

But typically, however, the victim has no relationship with that bank that is the beneficiary bank, because it's the fraudster's bank, not the victim's bank. The beneficiary bank owes that victim no common law duty of care because they're not a customer. And then there are also some standing and causation arguments that can be raised. There's not many circumstances where common law claims can be successful against the banks.

Within the transaction itself, you need to turn to Article 4A of the UCC, which provides the framework for evaluating the liability of the parties to the financial transaction, and given the large sums of funds that flow through the world's financial fund transfer systems, the drafters of the UCC made a very conscious decision to use precise and detailed rules to assign responsibility and define the norms, allocate risks, and establish limits on liability rather than rely on flexible principles.

So those of you familiar with Articles 3 and 4 of the UCC governing negotiable instruments that have comparative fault principles, those comparative fault principles aren't in Article 4A. There's no gray area. Article 4A clearly sets forth the roles and responsibilities of the parties to a transaction that occurs by wire and sets forth the respective liability scheme. And so typically because 4A is so broad and sets forth so clearly how and which parties are liable for what, typically state law claims are preempted and displaced by the UCC. And so, unless a party can allege negligence by the bank that occurred outside of the four corners of the wire transfer transaction, there usually is what's called preemption. And so, if you have negligence that occurred either before or well after the wire transfer process, there are some circumstances where a claim could be appropriate, but these circumstances really are pretty rare. And again, as I said earlier, other common law defenses such as causation standing, can bar the claims.

Chris Willis:

So that's very interesting that you have this governing of these claims mostly by UCC Article 4A, and given the legal background, Mary, that you just gave us, what would you recommend that the banks do if they're in a pre-litigation situation, they figured out that one of these fraud schemes has occurred and they're involved in some way. How should they look at and analyze the wire fraud claims in the pre-litigation stage?

Mary Zinsner:

I usually encourage my bank and clients when these cases come in to take a close look at the claims and start categorizing them into the respective roles of the bank. So, the first claims are the claims against what is known, as Susan referred to, the originating bank, or sometimes it's called the receiving bank. And it's a little confusing to use those terms, but the originating or receiving bank is the bank that receives the wire transfer instruction from its customer and initiates the wire transfer to the beneficiary bank. So here a bank has a relationship with the customer, and usually there are contracts of deposit and other treasury management documents which define the obligations of each. So those documents really need to be reviewed to see what they say when the case comes in.

And so, claims against the originating or receiving bank are subject to UCC Section 4A2-202, and involve a two-step analysis. And the bank considers whether the wire was authorized under 4A-202-1. And if the wire was authorized by someone who was the designated signatory for the customer, even if they were duped by fraud, so an account manager receives one of those emails that Susan was referring to and is duped to send the wire to the wrong place, that is still an authorized wire under the UCC and the inquiry should end there and there can be no recovery by the customer.

If the wire was not authorized, then you go to the second inquiry under 4A-202-2. Even if the transfer itself was not actually authorized by the customer, the bank may escape liability if it verified the transfer according to commercially reasonable procedures upon which the parties agreed to beforehand. Then that language, commercially reasonable procedures, is why claims under 4A-202 are a little harder to shake on a motion to dismiss, and they pose more risk to banks because sometimes complaints are pretty well pleaded because lawyers know how to craft a complaint to get it passed a motion to dismiss. And going through discovery itself can be expensive and delve into a bank's security processes, which is something you really always want to avoid, because the more the world understands about the bank's security processes, the more risk the bank is at to hackers. So, you need to be careful about limiting discovery to the bare minimum the customer or the victim needs to know and keeping everything under protective order.

And then the second category of claims are causes of action asserted against the beneficiary bank, the bank that receives the wire and credits to the account of the beneficiary, usually its customer and usually the fraudster. Usually, the allegation is that there is a mismatch between the beneficiary name and the account number. The plaintiff's claim that the bank should have seen the mismatch of the account name and the account number and caught the discrepancy. But under the UCC, the beneficiary bank is entitled to rely on the account number and is not obligated to detect a beneficiary account name/number mismatch. The only caveat to that is if the beneficiary bank has actual knowledge that the beneficiary is not the owner of the account identified in the wire transfer order. And this would be very unusual for a bank to have this actual knowledge, given that wire transfers occur in a matter of seconds. And once it receives the wire, the beneficiary bank typically credits the funds to the account of the beneficiary in under 30 seconds. So once the bank accepts the wire and credits the account of its customer, the wire transfer cannot be undone.

So, when we see claims against beneficiary banks, it's usually no cause for alarm. They don't pose significant exposure to banks because the party suing is not usually a customer, and the types of claims that can be asserted are pretty limited. The wire goes exactly as the sender directed to the fraudster's account, and the sender can't recover for this reason. And we've had a lot of success getting these claims against beneficiary banks dismissed on motions to dismiss.

I usually tell banks to take a look at which category the claim falls in. Is the bank a receiving bank, i.e. did it receive the wire from a customer? Or is it a beneficiary bank? And that determines the strategy in a case.

And then the other tip I'll offer is that when a lawsuit comes in or a pre-litigation demand comes in and you're the bank evaluating it, I like to spend a little time explaining the law to counsel for the plaintiff and inform them that the case is not likely to result in a recovery from the banks involved. Educating counsel if they're willing to listen is often a good way to get rid of these cases. No plaintiff's lawyer wants to spend a lot of time and invest a lot of money in a case where there likely will be no recovery. And I find a lot of plaintiff's lawyers really don't understand the applicable law and appreciate the education.

Chris Willis:

Got it. So having laid out those strategic considerations for the bank's pre-litigation, let's talk about the real world when the lawsuit is actually filed and being litigated. And Susan, I'd like to turn to you for this. When these cases get litigated, which they do pretty frequently, because the two of you handle a lot of them, how are the courts coming out on the types of issues that we just heard Mary talk about?

Susan Flint:

Well, I think you have to look at what Mary's talked about in terms of whether or not you're dealing with a beneficiary bank or the sending bank. And there are some solid cases out there for financial institutions, for their defense anyway, on wire claims, and one of them is the United States Court of Appeals for the Eleventh Circuit. It's really one of the few federal Circuit courts that analyzed the concepts of negligence and Article 4A in the context of a BEC fraud. And that case is called *Peter E. Shapiro, PA*, and it's a law firm that was involved in a closing of a sale transaction. That decision is unpublished right now, and I can read you the cite, 2019 U.S. App. LEXIS 35604 (11th Circuit, November 27th, 2019).

The case involved familiar parties to what we've been talking about. The two lawyers were involved in the closing and there were two banks involved in the wire transfer. The Florida lawyer was engaged by family members to handle the sale of a car dealership in upstate New York. He received payment instructions by email from the lender's lawyer, so from the other lawyer, directing that the wire of funds for the loan payoff be sent to a bank account in New York. Then the Florida lawyer received another set of wire instructions. It was purported to be from the same lender's lawyer, but was actually from the fraudster, and this time it directed the wire funds to a different bank instead. The Florida lawyer did not question that second fraudulent set of new instructions and did not verify that the new information was from the lender's lawyer. He thought it was, clearly. So, using those fraudulent instructions, he directed the bank to wire over $500,000 to the fraudster's account.

The bank receiving the wire transfer and processing it relied on the account number, notwithstanding that there was a name mismatch in the wire between the beneficiary name and the name on the account that received the wire funds. But as Mary just pointed out, the receiving bank cannot be held responsible for a beneficiary name mismatch generally, because they're not aware of any fraud that's occurring on the account.

The Florida lawyer, however, sued the bank alleging that it should not have processed that wire because the owner of the account that was identified on the payment order was not the beneficiary of the wire transfer as they identified it when they sent it. He asserted claims of common law negligence and violation of Florida statute codifying UCC Article 4A, which is the analysis, again, that Mary just went through for us.

The Florida statute adopted Article 4A and stated expressly that if the beneficiary's bank does not know that the name and the account number on the wire refer to different persons or different companies, it may rely on the account number as the proper identification of the beneficiary of the order. And the reason for that is, again, partly what Mary talked about, the numerous volume of wires. I mean, it's a phenomenal number of wires that go through the system every day. And the drafters of the uniform commercial code basically said this: If we stop wire transfers in this manner, we would have a huge impact on commerce. And that is not something that we want to do in terms of assigning liability at this point.

So, the Florida statute and Article 4A expressly says that if the beneficiary's bank does not know about the name and the number not matching or relating to different persons, it can rely on that account number. The district court then dismissed the common law negligence claim on preemption grounds and granted summary judgment for the bank on the Article 4A claim. The Eleventh Circuit affirmed the lower court's decision. The Eleventh Circuit found that Article 4A also displaced a common law negligence claim, given that it specifically defines the duties and the rights and the liabilities of the parties, particularly in a misdescription of beneficiary case.

So they found that the lawyer's argument that the bank had a duty to refuse to accept the wire because of the misdescribed beneficiary conflicted with the express language of the UCC, and it provided that in cases involving payment orders that identify both the account name and the account number where the bank lacks actual knowledge that the account name and number do not match, the beneficiary may rely on the number as proper identification for the beneficiary of the order. And that's what happened in the *Shapiro* case.

Chris Willis:

So that sounds like a vindication of the legal principles that Mary had told us about. The two of you have talked for a while about the liability of the two banks involved in a wire transfer. But how about in cases between the non-bank parties to the wire. Who bears the responsibilities among them, Susan?

Susan Flint:

That is a very good question, because we're starting to see a lot more of those types of cases. They're not just financial institutions anymore, and I think partly that's because financial institutions and the public, customers, are getting more knowledgeable about fraud, particularly in the email context. And so, we're seeing it in other arenas between different parties. It's more difficult to determine liability in those circumstances because there are no bright lines. There's no specific rules that govern who's going to be liable in these situations. But generally the loss is going to fall on the party that had the best opportunity to avoid the loss. So, the courts will examine the specific facts of each case, including red flags missed and a BEC scheme systems failures for the parties involved, and then they'll look at issues of comparative fault.

So, an example of this is case out of the Eastern District of Virginia called *Bile v. RREMC, LLC*, where the district court applied the UCC and contract theories and concluded that the wire transfer of settlement proceeds to the fraudster's account constituted payment under a settlement agreement. Plaintiff's lawyer was on notice that his account had, in fact, been hacked and he should have advised defense counsel of a possible attempt to misdirect the funds. So basically the court indicated that the loss was going to fall on the party that had the best opportunity to avoid the loss. And in that case, this was the plaintiff's lawyer.

There's also another case out of the U.S. Court of Appeals for the Sixth Circuit, which took a similar approach. That case is *Beau Townsend Ford Lincoln Inc. v. Don Hinds*. In this case, the seller, Beau Townsend Ford, transacted to sell 20 Explorers for about $740,000. The seller's email was hacked. The purchase funds transmitted by the buyer were misdirected. The buyer received the Explorers, but Beau Townsend Ford never received its payment. Beau Townsend Ford sued the buyer for nonpayment. The district court granted summary judgment on a breach of contract claim against the buyer, but the Sixth Circuit reversed and remanded, holding that the determining factor is whether either party's failure to exercise ordinary care contributed to the hacker's success. That might result in apportioning the loss by comparative fault.

So, because one party's email got hacked, it would carry, according to this analysis, some additional loss, or maybe all the loss. It depends. So, they remanded that case, but the parties subsequently settled the case, so we don't have an ultimate result on that case.

Chris Willis:

Let's go back to the point that we started the podcast on, which is we've talked about the legal principles, but we still know that wire transfer fraud schemes are prevalent and continue to be prevalent. It's a huge problem that's not going away. And so given that, Mary, banks certainly need to be aware of what's going on and take appropriate steps to protect themselves from these sorts of situations. What tips can you offer bank in-house lawyers in dealing with these kinds of wire transfer fraud situations?

Mary Zinsner:

These tips are not just for bank in-house lawyers, but really for all in-house lawyers in all industries, because wire fraud really is directed at every single industry these days. To start with, just stay vigilant and take precautions. The best steps parties can take to avoid losses are precautionary and educational to employees rather than reactionary. So really the first tip I'll start with is verify information, even from trusted sources. And don't use email to verify. Your employees should be placing verification calls to parties using phone numbers found in business records rather than those provided in an email, which could be fraudulent, and confirm the authenticity of instructions verbally, not by email. In most wire cases, the losses could have been avoided if the party sending the wire had verified the wiring instructions orally with a true trusted partner, rather than rely on email.

And then secondly, be extra vigilant if wiring instructions change. Fraudster's target emails with wiring instructions, and then send a modified email with updated directions for wiring money into their personal account. And also, be wary of instructions about wire transfers coming from a free email service, such as Gmail or Yahoo.

Another tip is to educate employees to double check email addresses providing wire instructions and look for slight variations, such as hyphens or underscores. Fraudsters usually use alias accounts with slight modifications so that the emails appear they are coming from a trusted partner. Susan pointed out a couple of these examples in her opening comments. Fraudsters like to use a hyphen or an underscore or something really simple that is easily overlooked. Be suspicious of wires going to an account with a geographic location different than the seller or party receiving the funds. If the closing transaction and the seller receiving the funds lives in Freeport, Maine, and a bank account is identified as the beneficiary bank as a branch in Miami, Florida is provided, ask questions about the closing transaction. There certainly could be possible explanations for locations which vary, but this is a red flag that should be explored, and it shouldn't be explored via email, it should be a phone call.

Customers should consult with their financial institutions and make sure they understand and have the processes and procedures in place and security protocols necessary to prevent wire fraud before wires are transmitted.

You also need to consider whether there's any applicable insurance coverage. When renewing your insurance coverage, explore whether your insurance program includes coverage for social engineering fraud. If it doesn't, ask your insurer if they offer business email compromise coverage for an additional premium. Check the language of the policy closely, as insurers

sometimes deny coverage for business email compromise losses on grounds that it was not the direct result of the use of the computer.

Really important is that companies and financial institutions of all sizes should know how to reach the local FBI field office, who can assist in freezing funds and tracking fraudsters. When you are defrauded, your first call is to your bank so they can attempt to claw back the wire. But the second call should be the FBI. I want to direct everybody to the website www.ic3.gov. It's a FBI website which tracks wire fraud, 24/7, monitors incidents 24/7. And by immediately entering information about the wire incident, it can immediately result in recovery of the funds.

And finally, if you are in-house counsel to a bank and regularly see wire fraud cases, start categorizing the cases and evaluating what role your bank played in the transaction. It helps determine strategy and any exposure. So those are our tips. If you have any questions, feel free to reach out to any of us, and I'll send it back to you, Chris, for the wrap up.

Chris Willis:

Okay. Thanks a lot, Mary. And Susan, thank you as well. Your insights on this podcast have been incredibly thorough and very informative, and I'm sure the audience will appreciate them. And of course, thanks to our audience for listening in to today's episode as well.

Don't forget to visit our blog, consumerfinancialserviceslawmonitor.com, and hit that subscribe button so that you can get our daily updates about the CFS industry and everything going on in it. And head on over to troutman.com and add yourself to our consumer financial services email list so that you can get our alerts and invitations to our industry webinars. And of course, stay tuned for a great new episode of this podcast every Thursday afternoon. Thank you all for listening.