KRISHEL LAW FIRM
Daniel L. Krishel, Esq. (SBN 149633)
4500 Park Granada, Suite 202
Calabasas, CA 91302
(818) 883-8759

Attorney for Plaintiff ALICE FRIES

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA, WESTERN DIVISION

ALICE FRIES Plaintiff, v. WELLS FARGO BANK, N.A. and DOES 1-100 Defendants.	CASE NO. 2:23-CV-07321-SPG-PD Hon. Sherilyn Peace Garnett **FIRST AMENDED COMPLAINT FOR DAMAGES** **JURY TRIAL DEMANDED (JURY DEMAND PREVIOUSLY FILED)**

Plaintiff alleges as follows and demands a trial by jury pursuant to the jury demand previously filed:

1. Plaintiff, ALICE FRIES (hereinafter "FRIES" or "Plaintiff ") is a resident of Los Angeles County, California and all acts complained of herein, occurred in Los Angeles County.

2. Defendant WELLS FARGO BANK, N.A. ("WF") is a bank chartered under the laws of the United States with headquarters located in California.

3. The true names and capacities, whether individual, corporate, partnership, associate, or otherwise, of defendants DOES 1 through 100, inclusive, are unknown to Cross Complainant, who therefore sues these defendants by such fictitious names. Cross Complainant is informed and believes and therein alleges that each DOE defendant herein is

4. Plaintiffs are informed and believes, and based upon this information and belief alleges, that each Defendant is, and at all relevant times was, the agent, servant, employee, and/or co-conspirator of the other Defendants, and that each defendant and unnamed co-conspirator was acting within the course and scope of his or its authority as the agent, servant, employee, and/or co-conspirator of the other Defendants; that each Defendant is jointly and severally liable to Complainant for the damages sustained as a proximate result of his or its conduct and that each and every act or omission of any defendant herein was ratified, expressly and/or impliedly, by each of the other Defendants herein. Therefore, Defendants refers to all Defendants in this complaint, named or unnamed, collectively, as "Defendants."

WELLS FARGO SECURITY PROCEDURES' AND AGREEMENT TO CONFIRM "AUTHENTICITY" OF WIRE TRANSFER PAYMENT ORDERS

5. Plaintiff Fries established a banking relationship with Defendant WELLS FARGO BANK ("WF") in or about 1986. Fries thereafter established her online banking access pursuant to the security procedures in place and set up by WF. From time to time, WF modifies its "Online Access Agreement" ("OAA") with periodic policy and procedures updates, and posts those updates on its website and/or emails those updates to its customers. The OAA and all of the online updates, detail some of the various security procedures in place and are the agreed upon means by which the authenticity of payment orders (wire transfer requests) issued to the bank in the name of the customer as sender, will be verified. Pursuant to *Commercial Code* 11202, payment requests deemed ***"authentic"*** are ***"effective"*** as the payment order of FRIES only if:

1) the agreed upon ***security procedure*** is a ***"commercially reasonable"*** method of providing security against unauthorized payment orders; and

2) ***the bank proves*** it accepted the payment order in ***good faith*** and;

3) ***in compliance*** with the ***security procedure***.

6. On or about February 15, 2022, WF posted the OAA which discusses some of the agreed upon security procedures. The OAA at paragraph 15(c) states that WF would use the security procedures described in the OAA "*and/or additional addenda*" and that the "purpose of the security procedure is to verify the authenticity of a transfer request delivered to" WF. At paragraph 18(b) the OAA confirms that WF would not be obligated to honor any transaction if it had "reason to believe" any such transaction "may not be authorized" by the customer whose authorization was necessary or if it was "not in accordance with any other requirement of our policies, procedures or practices" or if WF had "other reasonable cause not to honor" the requested transaction. FRIES uses WF's online platform, and therefore, agreed to these security procedures in the OAA and as amended/supplemented from time to time.

7. WF has at least three known security procedures in place to confirm a wire transfer payment order is authentic and therefore ***"effective"*** as the order of its customer:/1

1) WF will restrict the amount of money its customers can send online via a wire transfer payment order. WF specifically informs its customers in writing: **"*To request hire limits for online wires, please visit your local branch*."** As discussed below, anything above $50,000.00 is above the online wire transfer limit.

2) Wire transfer payment orders exceeding $50,000.00 will require a ***"secondary review"*** that will take 24-48 hours to complete before the funds will be sent to the designated recipient bank.

3) A more general security procedure used by WF on telephone conferences with customers is commonly known as "two factor authentication" ("2FA") in conjunction with security questions (the "2FA/security question procedure"). On this procedure, and during a phone call with a customer, WF sends a text message to the customer's cell phone and/or email address with a numeric code. The customer is then required to read back that numeric

---

1/ There may be other WF security procedures in place and once the deposition of WF is taken, those additional procedures will be revealed and a determination made as to whether any of those other procedures were violated along with the violations described in this complaint.

code to confirm the person is in fact, the WF customer they are purporting to be. After the code is confirmed, security questions are required to be asked by the WF representative, to which only the actual customer will have the answers. WF will not complete transactions until the "2FA/security question" procedure is successfully completed.

THE FRAUDULENT OCTOBER 24, 2022 WIRE TRANSFER PAYMENT ORDER

8. On October 24, 2022, at 1:10 p.m. FRIES placed a call to a WF "premier banker" who works out of the Hollywood branch, ("WF Advisor 1"). This person's direct WF' office line is 323-745-3096. FRIES told WF Advisor 1 during this four minute call the she (FRIES) would not be able to move forward with certain investments WF Advisor 1 had recently pitched. Upon hearing this, WF Advisor 1 expressed her disappointment and told FRIES that she had been working with two other WF associates (WF Advisor 2 and WF Advisor 3) and that the proposed investments should be pursued. FRIES again stated she was not interested in moving forward with any investments. After this brief four minute call ended, Ms. FRIES could hear WF Advisor 1 express her frustration to an unknown person and stated "I'm so sick of this."

9. Nine minutes after the call with WF Advisor 1 ended, at 1:23 p.m., FRIES received a phone call from an individual purporting to be a WF representative ("the WF Fraudster"). The fact that FRIES received a call from the WF fraudster just minutes after concluding her call with WF Advisor 1, proves either: 1) the WF fraudster is affiliated with or somehow connected to, WF and/or WF Advisor 1; or 2) it's one of the biggest coincidences in bank/wire fraud history. The "caller i.d." on FRIES' cell phone stated the call was coming from WF and listed the caller i.d. number as 800-225-5935 – which is an actual WF number as evidenced by the WF web site:

General Banking

Existing Accounts
1-800-225-5935

Mon – Sat: 7 am – 11 pm,
Sun: 9 am – 10 pm
Eastern Time

→ Mailing addresses
→ Contact us internationally
→ Make an appointment

The call by FRIES to WF Advisor 1 and the incoming call nine minutes later from the WF Fraudster to FRIES, are both confirmed in FRIES's cell phone bill:

Oct 24	1:10 PM	323.745.3096	Universal, CA	Lsan DA 14, CA	4
Oct 24	1:23 PM	800.225.5935	San Fernan, CA	Incoming, CL	60

The WF Fraudster told FRIES that her account had potentially been compromised and was exposed to fraudulent activity. The WF Fraudster sent a 2FA text to FRIES and told FRIES to read back the code so that FRIES could be verified as the actual customer. Because this exact scenario had played out numerous times before with a genuine WF representatives, FRIES had no reason to believe this 2FA scenario was any different or was in any manner, suspicious. FRIES received the code and read it back to the WF caller. FRIES spent the majority of this 60 minute phone call initiated by the WF Caller, on hold.

10. While on the phone with the WF caller, FRIES drove to a WF Santa Clarita branch to find out the status of her account. She was told by a WF employee ("Walter") to hang up her cell phone because it sounded like a scam. Walter told FRIES that funds were in the process of being wired out of her account ("the fraudulent wire transfer.") FRIES called the WF customer service line from the Santa Clarita branch phone as instructed by Walter. FRIES confirmed on this call, that she did not initiate nor authorize nor approve the wire transfer and that it needed to be recalled. FRIES was transferred to a WF representative named "Chavi" who confirmed the wire was recalled and gave FRIES a confirmation number. Chavi confirmed that the entire $100,000.00 would be back in FRIES' account

within 1-2 business days. The next day on October 25, 2022, FRIES contacted WF to check status of her account and when she could expect to receive the return of her $100,000.00. She was now told the wire was not recalled and that her money was sent to "Savage Car Wash" in Miami, Florida. After many conversations with different levels and departments, FRIES explained again and again, over and over, that she did not approve the wire and that she had a confirmation number for the recall. FRIES went to her local branch in Hollywood and again restated what occurred. On October 26, 2022, WF Advisor 1 sent an email to FRIES wherein WF Advisor 1 admitted the in-house WF investigator "is aware of this well-known scam."

11. For days, weeks and months thereafter, FRIES embarked on a futile attempt to get her money back – endless phone calls and in person appearances at WF' branch offices. WF told FRIES that unless she admitted in writing that she "authorized" the fraudulent $100,000.00 wire transfer, WF would not assist her in getting her money back. There was exactly zero legitimate or necessary reason for FRIES to make that false representation urged by WF, which was clearly an attempt by WF to shift liability from itself to FRIES. WF eventually sent an email to FRIES that it "regretted" any WF' "unsatisfactory service" and informed FRIES she would be receiving a "courtesy" credit to her account in the amount of $50.00 – which is $99,950.00 short of the $100,000.00 stolen out of her account as a direct result of the WF malfeasance described herein.

THE FRAUDULENT WIRE TRANSFER IS NOT AN "EFFECTIVE ORDER" AS TO FRIES

12. An October 24, 2022 phone call to WF that enabled the WF fraudster to induce WF to wire $100,000.00 from the FRIES account, was recorded by WF ("the wire fraud recording"). After this action was filed, FRIES obtained a copy of the wire fraud recording in which the conversation between the WF fraudster and the WF representative can be heard. The identity of the WF representative on this phone call cannot be ascertained at this time so he will be referred to as the "WF Mark." All WF security procedures were completely disregarded, ditched and thrown out the window by this utterly incompetent, WF employee.

13. **The fraudulent wire transfer payment order was not an "authentic" or *"effective order"* of FRIES for several separate and distinct reasons**:

1) it was not *in compliance* with the WF *security procedures for wire transfers*;

2) it was not in executed in *good faith* by WF;

3) the wire transfer procedures used on this transaction were not *"commercially reasonable."*

Therefore and because the fraudulent wire payment order is ***"not effective"*** as the order of FRIES, she is entitled to a full refund of the $100,000.00 fraudulent wire transfer payment order pursuant to *Commercial Code* Sections 11202(b), 11204(a).

FIRST CAUSE OF ACTION

Violation of Uniform Commercial Code–Funds Transfers [CA Commercial Code 11101 Et. Seq.; (UCC §4A-202)] –VIOLATION OF SECURITY PROCEDURES

Against WF and DOES 1-10

14. Plaintiff incorporates by reference paragraphs 1 through 13 as though set forth in full.

15. WF internal documents obtained after this action was filed, and the wire fraud recording itself, confirm the following time line of events occurred in the afternoon of October 24, 2022:

1) 1:24:30 the password to the FRIES online account was changed [by the WF fraudster].

2) 1:25:35 [the WF fraudster] logged into the FRIES on line account

3) 1:27:30 [the WF fraudster] enrolled the FRIES account into a wire transfer program known as "Wires Basic."

4) 1:31:11 [the WF fraudster] added a "wire payee" and attempted to wire from the FRIES account, $100,000.00 to Savage Car Wash.

5) 1:47:08: on a telephone call for the next 9 minutes and 44 seconds wherein nothing but superficial questions were asked by the WF Mark, the WF fraudster duped the WF Mark

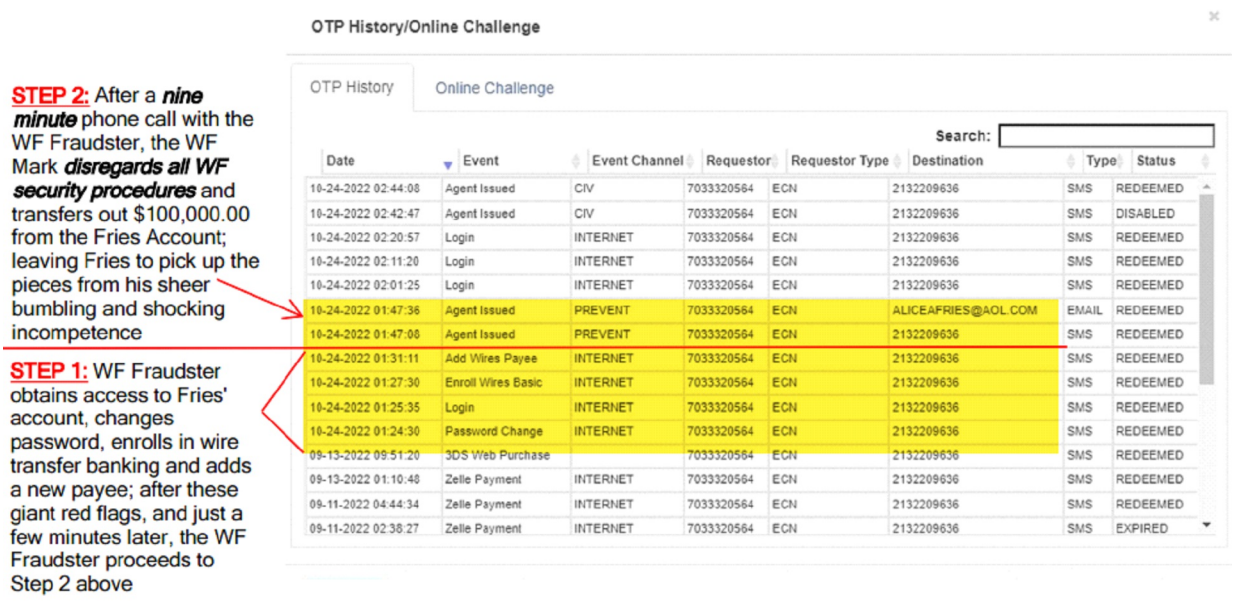
into wire transferring $100,000.00 out of the FRIES account to Savage Car Wash where those funds would never be seen again. FRIES has zero connection to Savage Car Wash and does not know any person affiliated with that business.

16. One of the security procedures implemented by WF is to reject online wire transfer requests from its customers if that request exceed a certain amount. The WF Mark confirmed in the wire fraud recording, the maximum online wire transfer request WF would accept, was $50,000.00. His statement on the wire fraud recording is consistent with the OAA as supplemented and amended on the WF website which specifically states: **"For your security, we restrict the amount of money you can send recipients online....*To request hire limits for online wires, please visit your local branch*."** The WF Mark further told the WF fraudster that the $100,000.00 online wire request was "an unusual amount of money" and that is why the FRIES account "had been flagged" and that any attempted transfer above $50,000.00 required a ***"second review"*** and that a delay of 24-48 hours could occur before the wire was sent.

17. **The wire fraud recording conclusively proves the WF Mark violated all three security procedures implemented by WF and described in paragraph 7 above:** The WF Mark was fully aware of the WF time line set forth above in paragraph 15 during his phone call with the WF fraudster and therefore, was fully aware the FRIES online password had just been changed (indeed, the WF Mark actually asked the WF fraudster if the password had just been changed); the FRIES "basic wire" ability had just been added and a new wire payee had just been added to the account as well. Incredibly, and despite all of these clear and unmistakable red flags, the WF Mark, in absolute and utter disregard of all known WF security procedures, told the WF fraudster: **"But no worries I'm going to release this wire transfer transaction and transfer it today."** He then stated: "I'm going to go ahead and authorize this transaction and have this released so that you, you or your brother will be able to receive it..." Seconds later the WF Mark stated: **"I would like to let you know that I already released the $100,000.00 on the wire that you initiated earlier."** And just like that, in a span of minutes, the funds were in fact released – in clear violation of all three

known WF security procedures: **1)** the second review that should have taken 24-48 hours was not implemented; **2)** requiring FRIES to visit in person, her local branch was not implemented; **3)** security questions were not asked as part of the 2FA/security question procedure: after the 2FA code was sent to the WF fraudster, an unknown voice can be heard in the background reading the 2FA code to the WF fraudster who then repeated it to the WF Mark – a massive red flag that the WF Mark failed to detect. Furthermore, the "security" questions asked by the WF Mark were absurd because he failed to ask any questions to which only FRIES would have known the answer. Instead, the WF Mark asked childish questions like: "Is your name Alice M Fries? "Can you tell me to whom are you sending the funds to?" And "you are sending the funds directly to Savage Car Wash?" and "Do you share your device with anyone?" Detailed personal questions about FRIES, not even a basic security rudimentary question like "what is your social security number" were ever asked.

18. Within minutes of the $100,000.00 fraudulent transfer payment order, FRIES realized what was happening and demanded WF cancel all wire transfers. If the WF Mark had complied with the WF security procedures, that $100,000.00 wire would have been cancelled and the funds never would have been sent. WF's absolute and clear violations of its security procedures allowed the fraudulent wire transfer to occur and directly caused Plaintiff's damages. The above recited sequence of events can be confirmed from the wire transfer recordings, and WF's own internally generated "OTP History/Online Challenge" it produced after this action was filed (See below and attachment Exhibit A):



19. When the WF Mark approved the fraudulent wire transfer payment order of $100,000.00 from the FRIES account, that payment order was not "authentic" and was ***not effective*** as a payment order from FRIES because WF did not comply with its own security procedures, in violation of *California Commercial Code,* section 11202(b)(ii), to wit: the WF Mark failed to reject the WF transfer payment order pending a "second review" for transfers exceeding $50,000.00 and he failed to require FRIES to visit a local branch before the transfer would be sent and he failed to implement properly, the security question/2FA procedure.

20. Per the express terms of Section 11202(b)(ii), WF has the burden to prove it complied with its agreed upon security procedures; based on the foregoing, it will be unable to do so. Therefore, the fraudulent payment order was ***not effective*** as to FRIES per *Commercial Code* 11202(b)(ii) and Fries is entitled to general damages, which includes but is not limited to, the full amount of the of the fraudulent wire transfer in the amount of $100,000.00 plus pre-judgment interest pursuant to Commercial Code 11204(a).

SECOND CAUSE OF ACTION

Violation of Uniform Commercial Code–Funds Transfers [CA Commercial Code 11101 Et. Seq.; (UCC §4A-202)] TRANSFER NOT MADE IN GOOD FAITH

Against WF and DOES 1-10

21. Plaintiff incorporates by reference paragraphs 1 through 20 as though set forth in full.

22. Based on all of the foregoing details set forth above and incorporated herein by reference, when the WF Mark on behalf of WF, wire transferred the funds out of the FRIES account, he did not do so in *good faith*, and instead chose to disregard all of the known WF security procedures described herein.

23. Per the express terms of Section 11202(b)(ii), WF has the burden to prove not only that it complied with its agreed upon security procedures, but that it *acted in good faith*; based on the foregoing, it will be unable to do so. Therefore, the fraudulent payment order was not effective as to FRIES per *Commercial Code* 11202(b)(ii) and Fries is entitled to general damages, which includes but is not limited to, the full amount of the of the fraudulent wire transfer in the amount of $100,000.00 plus pre-judgment interest pursuant to Commercial Code 11204(a).

THIRD CAUSE OF ACTION

Violation of Uniform Commercial Code–Funds Transfers [CA Commercial Code 11101 Et. Seq.; (UCC §4A-202)] SECURITY PROCEDURE NOT COMMERCIALLY REASONABLE

Against WF and DOES 1-10

24. Plaintiff incorporates by reference paragraphs 1 through 23 as though set forth in full.

25. Based on all of the foregoing details set forth above and incorporated herein by reference, the security procedure **actually implemented and used** by WF in the fraudulent

wire transfer at issue in this complaint, was not *"commercially reasonable."* The security procedure used by WF on **this particular transaction** consisted of ditching the "second review" for wire transfers exceeding $50,000.00; ditching the "in person" requirement for wire transfers exceeding $50,000.00; and ditching the security question prong of the 2FA/ security question procedure. Instead, the security procedure used by WF in **this transaction** (and not agreed to by FRIES) consisted of the pathetic and worthless nine minute telephone conference with the WF Mark described herein. The procedure actually implemented on this transaction, therefore, was not a *commercially reasonable security procedure* to authenticate the payment order, in violation of *Commercial Code* Section 11202(c) – *especially given the fact that FRIES had never before initiated a wire transfer*, let alone a transfer for $100,000.00, and given the fact that her password had been tampered with and changed minutes before the request was initiated, and that wire transfer capability had just been added. The "security procedure" actually used by WF on this particular transaction was *per se*, commercially unreasonable.

26. Per the express terms of Section 11202(b)(ii), WF has the burden to prove it complied with its agreed upon security procedures and acted in good faith and that its security was *commercially reasonable*; based on the foregoing, it will be unable to do so. Therefore, the fraudulent payment order was not effective as to FRIES per *Commercial Code* 11202(b)(ii) and Fries is entitled to general damages, which includes but is not limited to, the full amount of the of the fraudulent wire transfer in the amount of $100,000.00 plus pre-judgment interest pursuant to Commercial Code 11204(a).

//

FOURTH CAUSE OF ACTION

Violation of Uniform Commercial Code–Funds Transfers [CA Commercial Code 11101 Et. Seq.; (UCC §4A-202)] 2FA/SECURITY QUESTION PROCEDURE NOT COMMERCIALLY REASONABLE

Against WF and DOES 1-10

27. Plaintiff incorporates by reference paragraphs 1 through 26 as though set forth in full.

27. Pursuant to Commercial Code 11202(c) *commercial reasonableness of a security procedure* is a question of law to be determined by considering the wishes of the customer expressed to the bank, the circumstances of the customer known to the bank, including the size, type, and frequency of payment orders normally issued by the customer to the bank, alternative security procedures offered to the customer, and security procedures in general use by customers and receiving banks similarly situated. In this particular case, FRIES had never before initiated a wire transfer and did not even have wire transfer capability set up on her account.

28. The 2FA/security question procedure is not a commercially reasonable security procedure because it does not adequately provide security to insure payment orders are "authentic" – especially when used in conjunction with the weak and superficial "questioning" by persons like the WF Mark. WF is fully aware that the exact type of 2FA scam perpetrated against FRIES happens on a regular basis to its customers all over the United Sates. Nevertheless, WF continues to use this commercially unreasonable 2FA/security question system and has failed to undertake any steps to protect against payment orders that are not "authentic" with this failed and flawed system. Indeed, this case provides all the undisputed evidence needed to prove the commercially *unreasonableness* of the 2FA/security question system: in matter of just a few minutes, the WF fraudster was able to bypass the 2FA/security question system and was able to dupe the WF Mark, conclusively proving the 2FA/security question system is *per se*, *not* commercially reasonable by any

objective measure. And this exact same con-game is repeated over and over again all over the country and WF does absolutely, positively *nothing* to even try and stop it.

29. Per the express terms of Section 11202(b)(ii) WF has the burden to prove the 2FA/security question system is commercially reasonable; based on the foregoing, it will be unable to do so. Therefore, the fraudulent payment order was not effective as to FRIES per *Commercial Code* 11202(b)(ii) and Fries is entitled to general damages, which includes but is not limited to, the full amount of the of the fraudulent wire transfer in the amount of $100,000.00 plus pre-judgment interest pursuant to Commercial Code 11204(a).

FIFTH CAUSE OF ACTION

(Intentional Infliction of Emotional Distress

Against Wells Fargo and DOES 2-20)

30. Plaintiff incorporates by reference paragraphs 1 through 29 as though set forth in full.

31. Within minutes of becoming apprised of the wire transfer fraud, FRIES spoke to several WF employees on telephone calls in a desperate attempt to try and stop it. After this action was filed, WF produced some of those recorded telephone calls and some of them are described and summarized in this fifth cause of action. On one of these calls with WF "Employee 1" FRIES was placed on hold. While FRIES was on hold, WF Employee 1 made a separate (recorded) call to WF Employee 2 whom later identified himself as "Chavi." This WF recording revealed that the two WF employees discussed the FRIES wire fraud situation and the fact that the $100,000.00 wire had "already gone through." While FRIES was still on hold, the two WF employees discussed the fact that any successful attempt to recall the wire could not be guaranteed and that whether or not the wire could be successfully recalled was subject to an "online wire case" process that could take up to 120 days to complete.

32. Eventually, FRIES was added to the call between the two WF employees. Employee 1 left the call, leaving just FRIES and Employee 2 (Chavi) on the call. Despite knowing full well that it was probably too late to recall the wire and that the recall process

would take up 120 days to complete before anyone knew if the funds would be returned or not, Chavi affirmatively lied to FRIES and told her that wire transfer had been "stopped" and that he "stopped the wire" and that the funds would be back in her account and that she should check her online access to view the returned funds. FRIES was given a confirmation "wire stop" number of 0117845909 and told by Chavi that he was "sure the wire was not going to go through." When Chavi made these false statements on behalf of WF to FRIES that the wire had been "stopped" and that he was "sure the wire was not going to go through" he knew they were false because he and Employee 1 had just discussed the fact it would take up to 120 days and for the recall process to complete and it was entirely unknown if the wire could be successfully recalled or not.

33. Upon hearing the "good news" from Chavi that the wire had been successfully "stopped" and that the money would be back in her account in another day or so, FRIES was extremely relieved and felt like the entire day had been a bad, horrific nightmare.

34. As instructed by Chavi, FRIES checked her online account for the next couple days desperately looking for the return of her money; but it never appeared. She called WF yet again and was now told by yet another WF employee that the wire was not recalled and her money was gone. Upon hearing this news, FRIES was devastated, shocked and felt extreme, substantial and severe emotional distress after having been assured by Chavi that she would receive her money back in one or two days, and was now hearing from a different WF employee days later, the exact opposite.

35. WF's conduct in knowingly and intentionally lying to FRIES and falsely telling her that she would receive her money back in one or two days, knowing full well that was not going to happen, was extreme, outrageous and beyond the bounds of decency.

36. As if the foregoing was not bad enough, WF thereafter conditioned its assistance in getting her money back, only if FRIES first admitted in writing that she "authorized" the fraudulent $100,000.00 wire transfer. This was obviously done by WF to shield itself from its own actions, misconduct and liability. WF's demands that FRIES admit she authorized or verified the theft before it would even try to help her retrieve her funds –

knowing full well the funds were stolen from her – was further outrageous and intentional misconduct that it exceeds all bounds of decency in a civilized community.

37. WF's misconduct, first in lying to FRIES about the return of her money and then its coercive outrageous demand that she admit in writing that she authorized the wire transfer as a pre-condition to WF's assistance, are all are acts of misconduct outside the scope of the *Commercial Code* 11101 et. seq. and (UCC §4A-202)] and therefore, this cause of action is not displaced by these statutes as confirmed in *Zengen, Inc. v Comerica Bank* 41 Cal.4th 239 (2007).

38. WF's intentional misconduct as described herein, was outrageous and beyond the bounds of decency, oppressive, malicious and fraudulent thereby entitling Plaintiff to an award of general and punitive damages in amounts be determined at trial.

Plaintiff Prays:

ON THE FIRST, SECOND, THIRD, FOURTH CAUSES OF ACTION:

1. For general and special damages in an amount to be proven at trial in an amount of not less than $100,000.00, plus prejudgment interest.

ON THE FIFTH CAUSE OF ACTION:

2. For general and special damages in an amount to be proven at trial in an amount of not less than $100,000.00.

3. For punitive damages in an amount to be determined at trial.

ON ALL CAUSES OF ACTION

4. For costs of suit incurred herein;

5. For attorneys' fees permitted by law and the OAA.

6. For such other relief the court deems proper and appropriate;

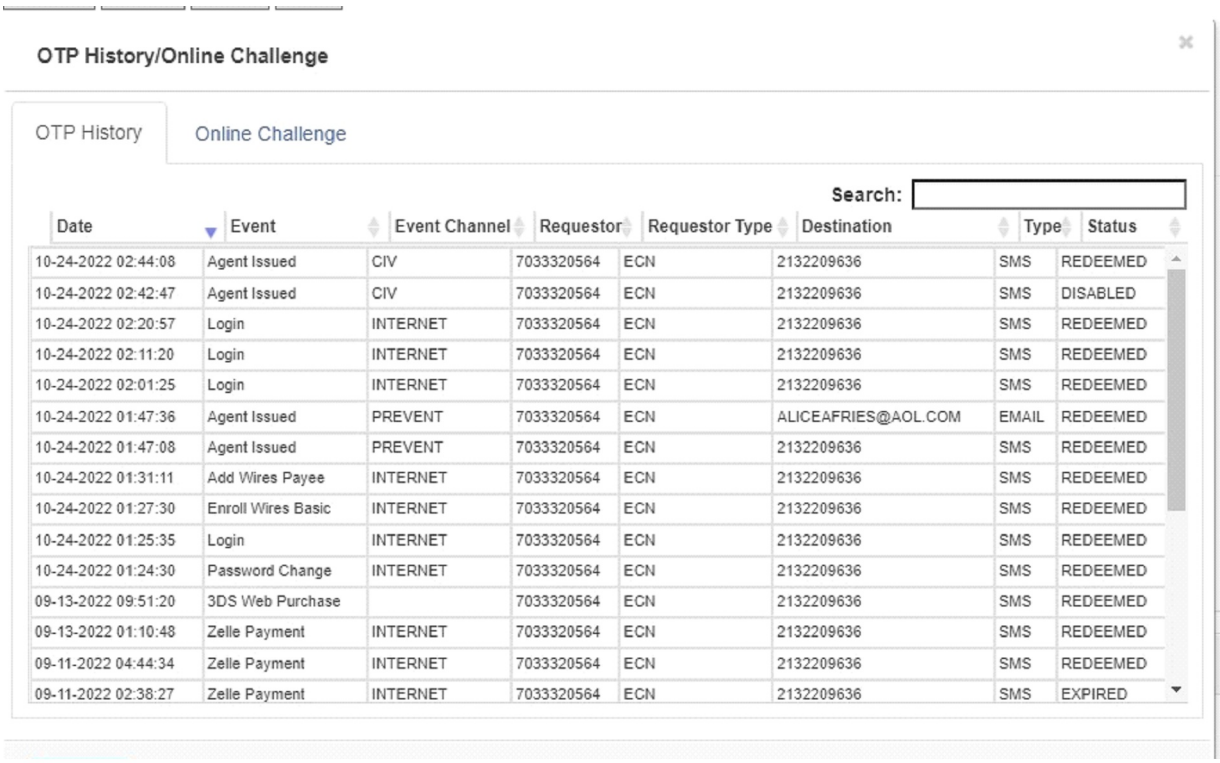
DATED: November 22, 2023

KRISHEL LAW FIRM

//Daniel Krishel

By:_____
DANIEL L. KRISHEL
Attorney for Plaintiff Alice Fries

A



OTP History/Online Challenge

OTP History | Online Challenge

Search:

Date	Event	Event Channel	Requestor	Requestor Type	Destination	Type	Status
10-24-2022 02:44:08	Agent Issued	CIV	7033320564	ECN	2132209636	SMS	REDEEMED
10-24-2022 02:42:47	Agent Issued	CIV	7033320564	ECN	2132209636	SMS	DISABLED
10-24-2022 02:20:57	Login	INTERNET	7033320564	ECN	2132209636	SMS	REDEEMED
10-24-2022 02:11:20	Login	INTERNET	7033320564	ECN	2132209636	SMS	REDEEMED
10-24-2022 02:01:25	Login	INTERNET	7033320564	ECN	2132209636	SMS	REDEEMED
10-24-2022 01:47:36	Agent Issued	PREVENT	7033320564	ECN	ALICEAFRIES@AOL.COM	EMAIL	REDEEMED
10-24-2022 01:47:08	Agent Issued	PREVENT	7033320564	ECN	2132209636	SMS	REDEEMED
10-24-2022 01:31:11	Add Wires Payee	INTERNET	7033320564	ECN	2132209636	SMS	REDEEMED
10-24-2022 01:27:30	Enroll Wires Basic	INTERNET	7033320564	ECN	2132209636	SMS	REDEEMED
10-24-2022 01:25:35	Login	INTERNET	7033320564	ECN	2132209636	SMS	REDEEMED
10-24-2022 01:24:30	Password Change	INTERNET	7033320564	ECN	2132209636	SMS	REDEEMED
09-13-2022 09:51:20	3DS Web Purchase		7033320564	ECN	2132209636	SMS	REDEEMED
09-13-2022 01:10:48	Zelle Payment	INTERNET	7033320564	ECN	2132209636	SMS	REDEEMED
09-11-2022 04:44:34	Zelle Payment	INTERNET	7033320564	ECN	2132209636	SMS	REDEEMED
09-11-2022 02:38:27	Zelle Payment	INTERNET	7033320564	ECN	2132209636	SMS	EXPIRED