

RETURN DATE: AUGUST 14, 2018

----- X	
PRECISION COMPUTER SERVICES, INC.,	: SUPERIOR COURT
	: :
Plaintiff,	: JUDICIAL DISTRICT OF ANSONIA-
	: MILFORD
-against-	: :
	: AT MILFORD
	: :
NEWTOWN SAVINGS BANK,	: :
	: :
Defendants.	: JULY 13, 2018
----- X	

COMPLAINT

Plaintiff Precision Computer Services Inc. (“PCS”), by its undersigned counsel, states the following as its Complaint against Defendant Newtown Savings Bank (“NSB”).

FACTS COMMON TO ALL COUNTS

1. Plaintiff PCS is a Connecticut corporation with a principal place of business in Shelton, Connecticut.
2. Defendant NSB is a Connecticut bank with a principal location in Newtown and locations throughout southwest Connecticut.
3. On March 6, 2017, PCS entered into a Wire Transfer Agreement with NSB (the “Wire Transfer Agreement”) (See Exhibit “A, which will be filed and served in accordance with Practice Book Section 10-29).
4. The Wire Transfer Agreement provides that only certain individuals at PCS identified as “Authorized Parties” were authorized to issue payment orders to NSB.
5. One of the “Authorized Parties” in the Wire Transfer Agreement is Michael FitzSimons of PCS.

6. On June 14, 2017, Ryan Storms, an Assistant Vice President and Branch Manager of NSB, received a fraudulent e-mail (the “Q Payment Order”) from an individual purporting to be Michael FitzSimons and which requested initiation of a wire transfer of \$67,560 from PCS’s account at NSB to a bank account in Hungary.

7. The e-mail was not in fact sent by Mr. FitzSimons but was instead sent by a fraudulent imposter (who was not an Authorized Party). The e-mail originated from an email address with a suffix of precisionqroup.com – which differs from PCS’s correct domain, which has a g instead of a q.

8. By altering one letter in the e-mail domain, the sender of the fraudulent e-mail employed a “spoofing” tactic of fraudsters that NSB, an institution engaged in the industry of banking, knew or should have known. Among other things, the tactic was set forth in an Email Fraud Advisory (FIN-2016-003) issued in 2016 by the Financial Crimes Enforcement Network of the United States Department of Treasury (FINCEN), which identified the following as suspicious behavior (among other things):

- *Transaction instructions originate from an e-mail account closely resembling a known customer’s e-mail account; however, the e-mail address has been slightly altered by adding, changing, or deleting one or more characters. For example:*

Legitimate e-mail address

- *john-doe@abc.com*

Fraudulent e-mail addresses

- *john_doe@abc.com*
- *john-doe@bcd.com*

9. NSB failed to identify the e-mail as fraudulent despite numerous red flags identified by FINCEN (and similar) guidance. The e-mail address differed from PCS’s address. The request

sought a transfer to a foreign bank account – a common destination of e-mail fraudsters, as would be known to a reasonably careful financial institution. Records available to NSB would have shown that PCS had never previously wired funds to Hungary, nor did it have any payment history or documented business relationship with the payee. NSB should have noticed that the Q Payment Order bore a time stamp of several hours after it was received by NSB – another indication that the e-mail originated from another part of the world. Furthermore, the Q Payment Order requested that payment be made “as soon as possible” – indicating urgency, another “red flag” for spoofing fraud.

10. NSB also failed to be appropriately suspicious about the e-mail originating outside the secure e-mail channel established between NSB and PCS.

11. Instead of flagging the Q Payment Order as fraudulent (as it should have through the use of reasonable care), NSB instead and as intended by the fraudsters forwarded the Q Payment Order to PCS’s comptroller (who, unlike NSB, had no reason or obligation to be knowledgeable about means and methods of financial fraud), and this ultimately led to an unauthorized transfer of \$67,560 from PCS’ account at NSB (the “Unauthorized Withdrawal”) to the fraudsters.

12. Promptly after it discovered that the fraud had occurred, PCS notified NSB that PCS did not order the fraudulent transfer.

13. None of the \$67,560 Unauthorized Withdrawal has been recovered by PCS.

14. Despite demand from PCS, NSB has declined to reimburse PCS for the amounts it withdrew in connection with the Q Payment Order and the Unauthorized Withdrawal.

COUNT I (BREACH OF CONTRACT – WIRE TRANSFER AGREEMENT)

1-14. PCS repeats and realleges Paragraphs 1 through 14 of the Complaint as if set forth fully herein and furthermore states as follows.

15. PCS entered into a Wire Transfer Agreement with NSB. PCS fully performed all of its obligations under the Wire Transfer Agreement. Pursuant to the Wire Transfer Agreement, only “Authorized Parties” were authorized to issue payment orders to NSB.

16. NSB made the \$67,560 Unauthorized Withdrawal in response to an order by a person or entity that was not an Authorized Party, in breach of the Wire Transfer Agreement entered into between PCS and NSB.

17. As a direct and proximate result of the breach of contract by NSB, PCS has suffered and will continue to suffer significant financial damages.

COUNT II (LIABILITY PURSUANT TO C.G.S.A. § 42a-4A-201, ET. SEQ.)

1-17. PCS repeats and realleges Paragraphs 1 through 17 of the First Count of the Complaint as if set forth fully herein and furthermore states as follows.

18. As set forth above, on June 14, 2017 NSB received a fraudulent payment order, the Q Payment Order, from an email address not associated with any Authorized Party pursuant to the Wire Transfer Agreement.

19. NSB improperly caused money to be transferred pursuant to the Q Payment Order, which was not sent or authorized by PCS or any agent of PCS.

20. Despite due and proper demand from PCS, NSB has failed to refund to PCS the Unauthorized Withdrawal in violation of C.G.S.A. § 42a-4A-204.

21. The Q Payment Order is not “effective as the order of [PCS]” pursuant to C.G.S.A. § 42a-4A-204(b). Any applicable agreements between PCS and NSB either: (a) failed to set forth

commercially reasonable methods of providing security against unauthorized payment orders; and/or (b) NSB failed to interpret and follow the agreements in a way that would have provided commercially reasonable methods of providing security against unauthorized payment orders.

More particularly:

- a. NSB did not (at least in the case of PCS) employ a practice of reviewing e-mail domain addresses to determine whether they actually originated from legitimate sources;
- b. NSB did not (at least in the case of PCS) follow guidance concerning fraudulent “spoofing” schemes (such as Email Fraud Advisory (FIN-2016-003)) and implement measures to guard against them;
- c. NSB did not undertake or follow any commercially reasonable obligation to verify a payment order;
- d. NSB did not include the use of algorithms, other codes, identifying words, numbers or encryption devices in verifying payment orders;
- e. To the extent NSB contends that mere receipt of an email instruction using a name of an authorized person is a security procedure, it is not a commercially reasonable method of providing security against unauthorized payment orders;
- f. The provision in the Wire Transfer Agreement that NSB “reserved the right to call on an Individual Authorized to Confirm a transfer request” is not part of a security procedure because NSB did not obligate itself to confirm the transfer request, it merely reserved the right to do so;
- g. NSB did not offer multi-factor authentication to PCS;

- h. NSB did not offer to PCS an IP block that would prevent orders originating from unapproved IP addresses;
- i. NSB did not detect and prevent the fraudulent transfer even though it was one of the largest ever from PCS's account, was directed to a bank in Hungary despite PCS having no transactions in Eastern Europe, and sent funds to an account to which NSB had never before transferred funds; and
- j. NSB failed to offer a dual control option under which two people must log in to complete a transaction; and
- k. NSB did not require communications concerning wire transfers to be initiated or occur through the secure e-mail channel.

22. To the extent that PCS will contend that NSB and PCS agreed that the authenticity of payment orders would be verified pursuant to a commercially reasonable security procedure, NSB did not accept the Q Payment Order in good faith and compliance with that security procedure. Among other things, NSB did not employ commercially reasonable means to determine whether the Q Payment Order actually originated from PCS, as alleged above.

23. The Q Payment Order was not caused directly or indirectly by a person who obtained access to the transmitting facilities of PCS or caused directly or indirectly by a person who obtained authority from PCS.

COUNT III (NEGLIGENCE)

1-14. PCS repeats and realleges Paragraphs 1 through 14 of the Complaint as if set forth fully herein and furthermore states as follows.

15. NSB had a duty to safeguard PCS's funds and to employ commercially reasonable security procedures to ensure that parties other than PCS would not be able to effect transfers of funds from PCS' accounts by fraudulent means. NSB also had a duty to train its employees concerning commercially reasonable means and methods to detect and prevent the type of foreseeable fraud which victimized PCS.

16. NSB breached these duties, proximately causing significant economic harm to PCS as described above.

COUNT IV (IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING)

1-14. PCS repeats and realleges Paragraphs 1 through 14 of the Complaint as if set forth fully herein and furthermore states as follows.

15. By accepting PCS' deposits and the fees paid the NSB for banking services, PCS entered into an implied contract with NSB whereby NSB agreed that it would safeguard PCS' deposits, including against fraudulent transfers.

16. By failing to employ proper security procedures to prevent the fraudulent transfer of PCS' funds as described above, NSB breached the implied covenant of good faith and fair dealing.

17. As a direct and proximate result of the breach of contract by NSB, PCS has suffered and will continue to suffer significant financial damages.

COUNT V (BREACH OF FIDUCIARY DUTY)

1-14. PCS repeats and realleges Paragraphs 1 through 14 of the Complaint as if set forth fully herein and furthermore states as follows.

15. PCS placed a unique degree of trust and confidence in NSB based upon NSB's superior and knowledge and skill in safeguarding money.

16. As PCS' bank, NSB owed fiduciary duties to PCS that included, without limitation, the duties to safeguard PCS funds and employ proper security procedures to ensure that parties other than PCS would not be able to effect transfers of funds from PCS' accounts by fraudulent means.

17. By failing to safeguard PCS funds and employ proper security procedures to prevent fraudulent transfer of PCS funds as described above, NSB breached its fiduciary duties to PCS.

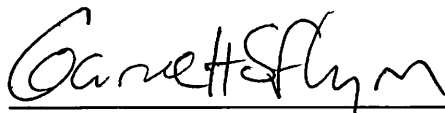
18. NSB's breach of fiduciary duties has caused significant economic harm to PCS as described above.

WHEREFORE, PCS demands:

1. Fair and just money damages;
2. Costs and interest;
3. Such other just and equitable relief as to which it is entitled.

Respectfully submitted,

PRECISION COMPUTER SERVICES INC.



By: Garrett S. Flynn, Esq. (Juris #418009)
LAW OFFICES OF GARRETT S. FLYNN, LLC
10 North Main Street, Suite 221
West Hartford, CT 06107
(860) 676-3148
gsf@flynn-law.com

Its Attorney

RETURN DATE: AUGUST 14, 2018

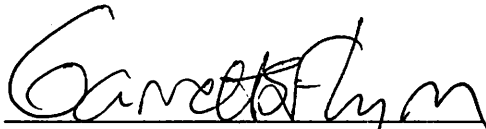
-----	X
PRECISION COMPUTER SERVICES, INC.,	: SUPERIOR COURT
Plaintiff,	: JUDICIAL DISTRICT OF ANSONIA-
-against-	: MILFORD
NEWTOWN SAVINGS BANK,	: AT MILFORD
Defendants.	: JULY 13, 2018
-----	X

STATEMENT OF AMOUNT IN DEMAND

The Plaintiff claims that the amount in controversy is more than two thousand five hundred and 00/100 (\$2,500.00) dollars, not including interest and costs.

Respectfully submitted,

PRECISION COMPUTER SERVICES INC.



By: Garrett S. Flynn, Esq (Juris #418009)
LAW OFFICES OF GARRETT S. FLYNN, LLC
10 North Main Street, Suite 221
West Hartford, CT 06107
(860) 676-3148
gsf@flynn-law.com

Its Attorney