**UNITED STATES DISTRICT COURT**
**SOUTHERN DISTRICT OF FLORIDA**

**CASE NO. 17-60907-CIV-MORENO/SELTZER**

FEDERAL TRADE COMMISSION, et al.,

Plaintiffs,

v.

JEREMY LEE MARCUS, et al.,

Defendants.

---

**PNC'S MOTION FOR PROTECTIVE ORDER**

Non-party PNC Bank, N.A. ("PNC") respectfully moves the Court, pursuant to Rule 26(c) of the Federal Rules of Civil Procedure and Local Rule 26.1(g)(3), for the issuance of a confidentiality agreement and protective order to limit the use and disclosure of confidential information the Court has ordered PNC to produce. PNC certifies that it has conferred with the Receiver, Jonathan E. Perlman (the "Receiver"), in an attempt to resolve this dispute without involving the Court, but the Receiver does not stipulate to the Confidentiality Agreement and proposed Protective Order ("PNC's proposed order") drafted by PNC. A copy of PNC's proposed order is attached to this instant Motion as Exhibit A.

**FACTUAL BACKGROUND**

On May 1, 2018, the Receiver issued a subpoena to PNC seeking 36 extremely broad categories of information. (*See* Doc. 357, p. 25). On May 18, 2018, PNC responded to the Receiver's subpoena. (*See* Doc. 363-1, Ex. A). On April 2, 2019, nearly a year after issuing his subpoena, the Receiver filed a Motion to Compel PNC to comply with the May 1, 2018 subpoena. (Doc. 357). On June 3, 2019, only days before the scheduled hearing before Magistrate Judge Barry Seltzer on the Receiver's Motion to Compel, the Receiver filed a new case against PNC, *Perlman v. PNC*, Case No. 19-cv-61390, pending before Judge Rodney Smith.

On or about July 2, 2019, the Receiver agreed to the terms of a confidentiality agreement and protective order for the purposes of receiving documents from PNC in this action, and the parties filed a Stipulated Confidentiality Agreement and Proposed Protective

Order with the Court. ("Stipulated Agreement") (*See* Stip. Confidentiality Agreement & [Proposed] Protective Order, Doc. 391, attached hereto as Exhibit B). The next day, on July 3, 2019 the Receiver withdrew the Stipulated Agreement, "[i]n order to incorporate additional input from the Federal Trade Commission, and the office of the Attorney General, State of Florida, Department of Legal Affairs." (*See* Notice re: Stipulation of Withdrawal of Stip. Confidentiality Agreement and [Proposed] Protective Order, Doc. 392). Another confidentiality agreement and proposed protective order was not filed.

On October 10, 2019, Magistrate Judge Seltzer entered a Report and Recommendation to deny the Receiver's Motion as untimely under the Local Rules, and because the Receiver could access the same information sought by the Subpoena in the new lawsuit through ordinary discovery procedures. (*See* Doc. 380). On October 15, 2019, Judge Moreno adopted Magistrate Judge Seltzer's Report and Recommendation in part, and ordered PNC to produce (1) the Receiver's requested documents "evincing communications between [PNC] and third-parties regarding the Defendants" and (2) "[PNC]-generated investigation reports of the Defendants." (*See* Doc. 427). As to the reports, the Court found that, "[t]o the extent these reports and the underlying assets allow the Receiver to recover and prevent dissipation of assets, they are related to the goals of this litigation." (*Id*. at 2). The October 15, 2019 Order further stated that "PNC Bank may provide the Receiver with a privilege log to the extent the documents are privileged under the Bank Secrecy Act." (*Id.* at 2-3).

PNC is continuing the process of searching for documents, if any, regarding communications between PNC and other financial institutions regarding the Defendants. If PNC locates any such documents, it will produce them.

PNC has located internal investigation reports regarding the Defendants and their closed accounts, generated in the course of PNC following its anti-fraud and anti-money laundering ("AML") processes and procedures. Some or all of these reports, as opposed to the underlying ordinary bank documents such as checks, will be withheld and noted on a "privilege log," consistent with the Court's October 15, 2019 Order and the confidentiality requirements of the Bank Secrecy Act, 31 U.S.C. § 5318(g)(2), because they reflect whether a Suspicious Activity Report ("SAR") was or was not filed. *See Shapiro, P.A. v. Wells Fargo Bank, N.A.*, No. 18-60250-CIV-HUNT, 2018 WL 4208225, *1 (S.D. Fla. July 23, 2018) (denying motion to compel non-SAR documents that state whether a SAR was or was

not filed). None of these reports shed light on the ability of the Receiver to recover or prevent the dissipation of assets, or the potential liability of third parties other than the named Defendants in this action.

However, all of PNC's documents are entitled to confidentiality. Specifically, these documents—generated so that PNC may comply with its obligations under the Bank Secrecy Act ("BSA"), including determining whether to file SARs with the government—contain highly confidential and sensitive information that, if publicly disclosed, would result in unnecessary harm to PNC and more generally to the AML and anti-fraud goals of the BSA. PNC therefore requests the entry of a confidentiality or protective order in the form attached as Exhibit A. *See* Fed. R. Civ. P. 26(c).

The deadline to produce the documents under the Court's Order is November 13, 2019. The parties have met and conferred and the Receiver indicated that, despite having previously agreed to the same form of order, he objects to the entry of the proposed protective order, necessitating the filing of the instant motion. PNC will provide *ex parte* to the Court the documents responsive to the October 15, 2019 Order this week. Once the Court adjudicates this motion, PNC will turn over the responsive documents and a privilege log to the Receiver consistent with the Court's Orders.

**LEGAL STANDARD**

It is well settled that a court may issue a protective order "for good cause to preserve the confidentiality of sensitive materials and regulate access to the information pursuant to Federal Rule of Civil Procedure 26(c)(1)(G)." *Rubenstein Law*, 2017 U.S. Dist. LEXIS 11240, *4 (M.D. Fla. Jan. 27, 2017) (citing *In re Alexander Grant & Co. Litig.*, 820 F.2d 352, 355 (11th Cir. 1987)). In determining whether good cause exists to enter a protective order, courts in the Eleventh Circuit apply a four factor test, which includes: "(1) the severity and the likelihood of the perceived harm; (2) the precision with which the order is drawn; (3) the availability of a less onerous alternative; and (4) the duration of the order." *Gunson v. BMO Harris Bank, N.A.*, 300 F.R.D. 581, 583 (S.D. Fla. 2014) (citing *In re Alexander Grant & Co. Litig.*, 820 F.2d 352, 356 (11th Cir. 1987)).

## ARGUMENT

### 1. The Severity and Likelihood of Harm Is High If the Proposed Order Is Not Entered

Ample good cause exists to enter PNC's proposed order because the documents the Court has ordered PNC to produce are sensitive and confidential business records that, if publicly revealed, would result in unnecessary harm to PNC and more generally to the AML and anti-fraud goals of the BSA. In particular, the alerts and reports generated by PNC's proprietary AML program are highly confidential, particularly because they are intrinsic to PNC's process of determining whether to file a SAR in regards to potentially suspicious activity. Disclosing details concerning PNC's AML and fraud detection and prevention documents without a confidentiality order in place raises concerns not only for PNC, but also for the financial industry as a whole.[1]

PNC's fraud detection and prevention procedures are highly tailored and are part of PNC's complex internal systems it uses to detect and investigate potentially illegal activity. The law and sound banking practices require such procedures. Foregoing a confidentiality agreement and protective order in this case could lead to aspects of non-party PNC's anti-fraud strategy falling into the wrong hands, resulting in harm to PNC, its customers, and other financial entities that employ similar procedures. Therefore, it is imperative that PNC's investigative reports that give insight into PNC's fraud detection and AML programs remain confidential.

Because courts protect proprietary business interests (especially those of a non-party such as PNC), courts should extend the same—if not greater—protections when the risks presented by disclosure threaten to undermine systems designed to prevent and detect potential criminal or fraudulent activity. Accordingly, because courts are aware of the risks that disclosure in discovery can pose to institutions that possess highly personal and/or valuable information, courts have issued protective orders to protect an entity's security and fraud prevention documents. *See e.g., Dubai Islamic Bank v. Citibank, N.A.*, 211 F. Supp. 2d

[1] To the extent communications between PNC and other financial institutions regarding the named Defendants in this action, if any, are located and produced, the same concerns would apply regarding the need for the proposed order, because PNC would not have occasion to communicate about its customers with other financial institutions unless the communications pertained to anti-fraud or loss prevention issues.

447, 448 & n.1 (S.D.N.Y.2001) (bank's AML and wire transfer security policies and procedures subject to protective order in discovery); *see also Dannenbring v. Wynn Las Vegas, LLC*, No. 2:12-cv-00007, 2013 WL 2460401, at *3-4 (D. Nev. June 6, 2013) (casino's internal security investigation procedures and processes subject to protective order); *Millwrights' Local 1102 Supp. Pension Fund v. Merrill Lynch, Pierce, Fenner & Smith, Inc.*, No. 07-15150, 2010 WL 2772443, at *3 (E.D. Mich. July 13, 2010) (internal documents relating to Merrill's ethics and conflicts policies subject to protective order); *The Bank of N.Y. v. Meridien Biao Bank Tanzania Ltd.*, 171 F.R.D. 135, 144 (S.D.N.Y. 1997) (BNY's internal audit procedures manual, credit policy manual, authorized signature book, and operations manual subject to strict protective order because unauthorized disclosure "would diminish BNY's competitive edge, confer on its competitors an unwarranted advantage in the industry, and furnish a potential avenue for fraud by third parties."); *Superior Edge, Inc. v. Monsanto*, Civil No. 12-2672, 2014 WL 7183797, at *3-4 (D. Minn. Dec. 16, 2014) (protective order for source code); *In re Anthem, Inc. Data Breach Litig.*, No. 15-MD-02617 ¶ 8 (N.D. Calif. Sept. 21, 2015) (D.E. # 293) (similar protections); *United States v. Xue*, No. 16-22 (E.D. Pa. Sept. 20, 2016) ¶ 2 (D.E. #108) (similar protections in a criminal trade secrets case).[2]

[2] Further, several other courts have found that sensitive data about company information, security policies and practices warrant heightened protection in litigation. *See, e.g., In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, No. 16-MD-027520LHK, 2018 U.S. Dist. LEXIS 48872, at *25-26 (N.D. Cal. Jan. 3, 2018) (granting motion to seal portion of complaint relating to (1) Yahoo's technology to provide services and security to its users because such disclosure could cause competitive harm; and (2) Yahoo's technology to protect its users' information, as well as methods previously used to breach the company's system, because such information "could be used by cyber-attackers to attempt to again hack Yahoo's systems"); *OneAmerica Fin. Partners, Inc. v. T-Systems N Am., Inc.*, No. 1:015-cv-01534, 2016 WL 891349, at *2-4 (S.D. Ind. Mar. 9, 2016) (public disclosure of IT system information of questionable relevance to litigation would provide a blueprint for exploiting financial services company's defenses against hackers, fraudsters and other criminals); *Music Grp. Macao Comm. Offshore Ltd. v. Foote*, No. 14-CV-03078 JSC, 2015 WL 3993147, at *5-6 (N.D. Cal. June 30, 2015) (finding a "compelling" reason to seal exhibits detailing company's network infrastructure and security systems and security incident investigative procedures); *EON Corp IP Holdings LLC v. Cisco Sys. Inc.*, No. 12-CV-01011-JST, 2014 WL1017514, at *2 (N.D. Cal. Mar. 11, 2014) (finding "compelling" reasons to seal documents that disclose "confidential technology, product configurations, security features, and network configurations"); *In re Google Inc. Gmail Litig.*, No. 13-MD- 02430-LHK, 2013 WL 5366963, at *3 (N.D. Cal. Sept. 25, 2013) (sealing information about users' interactions with the Gmail system based on Google's assertions that "hackers and spammers could use this

An analogy also may be made to more traditional law regarding the discovery of trade secrets and other proprietary information. Because courts have protected confidential information simply to protect proprietary business interests, courts should extend the same—if not greater—protections when the risks threaten to undermine systems designed to prevent and detect potential criminal or fraudulent activity. *See, e.g.*, *Corcel Corp. v. Ferguson Enters.*, 291 F.R.D. 680, 680-82 (S.D. Fla. 2013) (entering protective order to protect trade secret and commercially sensitive information).[3]

In contrast to the scenarios presented by the cases cited by the Receiver, the potential for compromise of PNC's fraud detection systems by disclosure of the investigative reports in the absence of a protective order should be viewed in the context of the threat environment in which

---

information to circumvent Google's [anti-fraud and security procedures]" and based on the limited relevance of the information); *Metavante Corp. v. Emigrant Sav. Bank*, 2009 WL 637165, at *1 (E.D. Wis. Mar. 11, 2009) (granting motion to seal email that appeared to contain "confidential information on specific types of software used by [defendant]").

[3] The Receiver has, in the context of his meet and confer requirement, brought to our attention three cases denying a request for a protective order. *See Abby v. Paige*, No. 10-cv-23589, 2011 U.S. Dist. LEXIS 162979 (S.D. Fla. Aug. 31, 2011); *Syncor Int'l Corp. v. Mody*, No. 98-6284, 2000 U.S. Dist. LEXIS 1020 (E.D. Pa. Feb. 4, 2000); *Mayfair House Ass'n, Inc. v. QBE Ins. Corp.*, No. 09-80359, 2010 U.S. Dist. LEXIS 149466 (S.D. Fla. May 6, 2010). These cases are readily distinguishable because they either involved deficient filings seeking confidentiality, or sought to protect information nowhere near as sensitive as that which will be found in the documents PNC is to produce. The Court in *Abby* denied the parties' jointly-proposed confidentiality order to protect information regarding defendant's net worth—which was submitted with no accompanying memorandum of law or statement of good cause—because the parties "[had] not shown good cause to justify their desire for secrecy." 2011 U.S. Dist. LEXIS 162979, at *2.[3] The parties in *Syncor* also "utterly fail[ed] to address any consideration under the required 'good cause' standard, . . . failed to show with any specificity that disclosure will cause a defined and serious injury and they articulate[d] no justification for requesting the Court to enter such an Order." 2000 U.S. Dist. LEXIS 1020, at *5. And in *Mayfair*, the defendant insurance company moved for a protective order so as to confidentially produce documents evidencing dates and payment amounts to insured condominium associations. 2010 U.S. Dist. LEXIS 149466, at *2. The Court denied the motion because, *inter alia*, defendant had publicly-disclosed the total payments made to the associations, and had not shown how disclosing the specific dates and payments would be materially different. *Id.* at *6-7. The Court also recognized defendant's interest in "keeping its business information as confidential as possible," but held that defendant had not "shown that any of the information is deserving of any protection." *Id.* at *8. These cases demonstrate nothing more than the readily known principles that information must be truly sensitive to be deserving of confidentiality, and that parties seeking such orders need to demonstrate good cause for entitlement to protection. PNC has satisfied both requirements here.

PNC and other financial institutions operate. Unprotected information could be accessed by bad actors, who then could use it to try to reverse-engineer PNC's anti-fraud and AML programs. As the United States Department of the Treasury noted in late 2016:

> The size, reach, speed, and accessibility of the U.S. financial system make financial institutions attractive targets to traditional criminals, cybercriminals, terrorists and state actors. These actors target financial institutions' websites, systems, and employees to steal customer and commercial credentials and proprietary information; defraud financial institutions and their customers; or disrupt business functions.

U.S. Department of the Treasury, FINCEN, "Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime," FIN-2016-A005 (Oct. 25, 2016), available at https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a005. Further, financial institutions like PNC are subject to heightened regulation as to information security and fraud prevention. Each financial institution is required to tailor its information security and anti-fraud program to address the specific risks that it faces. *See, e.g.*, FFIEC, FFIEC Information Security Booklet (Sept. 2016), available at http://ithandbook.ffiec.gov/it-booklets/information-security.aspx (requiring financial institutions to maintain effective security programs, tailored to the complexity of their operations).

Likewise, in order to mitigate the risk of third-party data breaches, the Office of the Comptroller of the Currency ("OCC") requires national banks such as PNC to ensure that the vendors and other third parties to whom banking information is sent have adequate security protections in place.[4] In its Spring 2018 Semiannual Risk Perspective (the "Report"), the OCC again emphasized banks face increasingly sophisticated cyber threats that "seek to exploit personnel, processes, and technology." OCC, Spring 2018 Semiannual Risk Perspective (June 2018), *available at* https://www.occ.treas.gov/publications/publications-by-type/other-publications-reports/semiannual-risk-perspective/semiannual-risk-perspective-spring-2018.pdf. Using data gathered through the FFIEC Cybersecurity Assessment Tool over two examination

[4] *See, e.g.*, OCC, Bulletin 2013-29, *Risk Management Guidance* (Oct. 30, 2013). In light of increasing concern over how the cybersecurity weaknesses of third parties could have a "systemic" impact on the financial system, federal banking regulators recently issued an Advanced Notice of Proposed Rulemaking on enhanced cybersecurity standards that would encompass "external dependency management" of "outside vendors, suppliers, customers, utilities, and other external organizations and service providers . . . ." *See Enhanced Cyber Risk Management Standards*, 81 Fed. Reg. 74315 (proposed Oct. 26, 2016).

cycles, the OCC has found that these threats target personal information and intellectual property "to facilitate fraud and misappropriation of funds at the retail and wholesale levels." Other threats seek to disrupt or otherwise impair bank operations.

The confidentiality and security of a bank's AML and anti-fraud program is critical to managing the very risks against which the program is designed to protect. The cases and regulations noted above highlight the increasing awareness among judges and the U.S. Government of the growing need to protect and prevent the public from viewing an institution's fraud prevention documents. PNC urges this Court to adopt its proposed order, which would protect it from suffering any undue harm, while also giving the Receiver access to the requested documents. PNC seeks only ordinary protections for its confidential business records.

**2. <u>The Proposed Order Is Narrowly Drawn and Proportional</u>**

PNC's proposed order is narrowly drawn and proportional because it (i) includes precisely drawn terms that allow sharing of the information, even including use in the new *Perlman v. PNC* case; (ii) recognizes confidential information may be required to be disclosed in certain contexts, and (iii) allows for challenges to confidentiality designations. For example, Paragraph 7 of the proposed order entitles the Receiver to use PNC's documents in the *Perlman v. PNC* case while also enabling the Receiver to share the confidential documents with counsel for the FTC and the State of Florida. In addition, paragraph 12 of the proposed order permits any party who is requested or required to disclose any confidential information to notify the party who designated the information as confidential so that, if needed, the party may seek an appropriate order or remedy. Lastly, paragraph 15 of the proposed order enables a party to challenge the designation of any material as "Confidential." Therefore, PNC's proposed order contains more than adequate provisions to ensure that the Receiver, the FTC, and the State of Florida have full access to the documents and that they do not suffer any harm from the issuance of the proposed order.[5] Conversely, if PNC's investigatory reports are disclosed without a confidentiality order in place,

[5] To the extent the FTC or the State of Florida objects to the issuance of an order in this case, they are not parties to the proposed order, and it was the Receiver (not the FTC or State) who requested the documents by subpoena. Indeed, by statute, the FTC cannot regulate or bring enforcement actions against banks—that is the sole province of the OCC. 15 U.S.C. § 45(a)(2). Regardless, the proposed order permits the Receiver to share documents with the FTC and State, so they cannot possibly suffer harm by its entry. Moreover, PNC has a strong interest in maintaining the confidentiality of the documents at issue, and there is a strong public interest in keeping AML-related investigative reports confidential.

PNC and the public interest goals of the BSA will suffer harm because aspects of PNC's anti-fraud and AML strategies would be publicly available thereby undermining PNC's efforts to prevent and detect illegal activity, and increasing the risk that PNC itself will be victimized by fraudulent conduct.

**3. No Less Onerous Alternative to PNC's Proposed Order Exists**

As discussed above, PNC's proposed order is the least onerous approach for the disclosure of the documents because it enables both the dissemination of discovery between counsel involved in the underlying case and the new *Perlman v. PNC* case. Thus, the proposed order protects the disclosure of PNC's confidential business information while allowing the Receiver to share the confidential documents with counsel for the FTC and the State of Florida; such an arrangement promotes the dissemination of discovery while also protecting PNC from suffering undue harm by complying with court-ordered document production.

Courts in this Circuit have granted similar requests for the issuance of a protective order. For example, in *Gunson v. BMO Harris Bank, N.A. et al.*, 300 F.R.D. 581 (S.D. Fla. 2014) the court granted the defendants' (who were numerous banking institutions) request for a protective order because the plaintiff sought, among other things, the defendants' internal audits, risk assessments, and details regarding electronic payment transactions with third parties. *Id.* at 583. The court found that issuing a protective order would "promote the prompt resolution of disputes regarding confidentiality and assist in the flow of discovery." *Id.* The court further found that the plaintiff had failed to demonstrate how she would suffer any harm by the issuance of a protective order permitting documents to be marked confidential. *Id.* Thus, courts in this Circuit do not disfavor issuing protective orders in cases involving sensitive and confidential documents belonging to financial institutions.

Additionally, the Receiver cannot show that he will suffer any harm if the proposed order is entered. Tellingly, the Receiver previously agreed to a confidentiality agreement and protective order. (*See* Stip. Confidentiality Agreement & [Proposed] Protective Order, Doc. 391, attached hereto as Exhibit B). The parties later withdrew this proposed order (*see* Notice re: Stipulation of Withdrawal of Stip. Confidentiality Agreement and [Proposed] Protective Order, Doc. 392), when the FTC and State expressed concerns regarding the impact the Order could have in their case against Jeremy Lee Marcus and the other defendants. Because the Receiver, the FTC and the State were unable to successfully confer, incorporate changes to the proposed order, and resubmit

it, a replacement proposed order was never filed. Notwithstanding this road block, PNC then agreed to voluntarily provide the Receiver with over 12,000 pages of transactional banking documents—documents which counsel for the Receiver told the undersigned that the Receiver still wanted—without the benefit of a protective order, in order to keep the process moving. However, the documents at issue in the Court's October 15, 2019 Order are fundamentally different than the previously-provided account records (which were properly redacted), because they are much more sensitive and implicate anti-fraud concerns.

In any event, the FTC's and State's apparent concerns are unfounded because, as noted above, the request for production of these documents was *not* propounded by the FTC or State; the FTC and State are not parties to the proposed order; and the proposed order allows the sharing of information between the Receiver and FTC and State. Additionally, Marcus and all other defendants have already entered consent final judgments with the FTC and the State of Florida, so there can be no legitimate concern that the proposed order would impact the FTC and State's case against Marcus and the other defendants—those matters are resolved and final orders have been issued as to all defendants. *See* Plaintiffs' Third Notice of Status Proceedings, Doc. 320, ¶ 1 ("Final orders have been entered against all defendants.") Therefore, the FTC's and State's apparent concerns are no longer valid.

Because issuing the proposed order will not harm the Receiver, the FTC, or the State of Florida, while disclosing such documents without a confidentiality order in place will result in undue harm to PNC as described above, PNC requests that the Court issue PNC's proposed order, which is identical to the version that the parties previously had filed with the Court.

**4. PNC's Protective Order Has a Limited Duration**

The proposed order has a limited duration. To PNC's knowledge it will only be used for the document production which PNC has been ordered to make. All other discovery will be done in connection with the *Perlman v. PNC* case. Further, the protective order only extends between the Receiver and PNC and not to the FTC or State of Florida.

## CONCLUSION

For the foregoing reasons, PNC requests that the Court enter PNC's proposed order as attached as Exhibit A to govern discovery in this case.

## LOCAL RULE 7.1(a)(3) CERTIFICATION

Counsel for PNC Bank has conferred with counsel for the Receiver in a good faith effort to resolve the issues raised in the motion and has been unable to do so. Specifically, the parties have met and conferred and the Receiver indicated that, despite having previously agreed to the same form of order, he objects to the entry of the proposed protective order, necessitating the filing of the instant motion.

Respectfully submitted,

s/*Peter D. Hardy*

Dated: November 4, 2019

Peter D. Hardy (admitted *pro hac vice*)
**Ballard Spahr LLP**
1735 Market Street, 51st Floor
Philadelphia, PA 19103
Telephone: 215.864.8838
HardyP@ballardspahr.com

Melanie J. Vartabedian (admitted *pro hac vice*)
**Ballard Spahr LLP**
One Utah Center
201 South Main Street, Suite 800
Salt Lake City, UT 84111-2221
Telephone: 801.531.3000
Vartabedianm@ballardspahr.com

Respectfully submitted,

s/*Peter W. Homer*

Dated: November 4, 2019

Peter W. Homer, Esq.
**Homer Bonner Jacobs, P.A.**
1441 Brickell Avenue
1200 Four Seasons Tower
Miami, FL 33131
Telephone: (305) 350-5100
PHomer@homerbonner.com

**CERTIFICATION OF SERVICE**

I hereby certify that, today, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will also send notice of this electronic filing to all counsel of record.

Respectfully submitted,

s/*Peter W. Homer*

Dated: November 4, 2019

Peter W. Homer, Esq.

# EXHIBIT

# A

**UNITED STATES DISTRICT COURT**
**SOUTHERN DISTRICT OF FLORIDA**

**Case No. 17-60907-Civ-Moreno/Seltzer**

FEDERAL TRADE COMMISSION, *et al.*

Plaintiffs,

v.

JEREMY LEE MARCUS, *et al.*,

Defendants.

---

**[PROPOSED] CONFIDENTIALITY AND PROTECTIVE ORDER**

WHEREAS, Jonathan E. Perlman, the Court-appointed Receiver ("Receiver") of the Receivership Entities in the above-captioned case, served PNC Bank, N.A. ("PNC") with a subpoena *duces tecum* on May 1, 2018 seeking production of documents (the "Subpoena"); and

WHEREAS, on April 2, 2019, the Receiver moved to compel production of documents responsive to the Subpoena (D.I. 357); and

WHEREAS, on April 29, 2019, PNC opposed the Receiver's motion to compel (D.I. 363); and

WHEREAS, on June 11, 2019 this Court denied the Receiver's motion to compel (D.I. 380); and

WHEREAS, the documents to be produced pursuant to the Subpoena contain financial and other sensitive information which may be confidential; and

WHEREAS, good cause exists for the entry of this Protective Order (the "Order").

NOW THEREFORE, upon entry by the Court pursuant to Rule 26(c) of the Federal Rules of Civil Procedure, the following Order shall govern the disclosure of confidential information from PNC to the Receiver in the above-referenced case, *Federal Trade Commission, et al., v. Jeremy Lee Marcus, et al.* 17-60907-Moreno/Seltzer, currently pending in the United States District Court for the Southern District of Florida (the "Action"). The Receiver and PNC are each a "party" and together, the "parties."

1. Scope of Order. All information disclosed pursuant to the Subpoena is subject to this Order and shall be deemed Confidential Information to the extent that it is designated as Confidential Information pursuant to this Order. Confidential Information shall not be used or disclosed to anyone except as provided in this Order. For the purposes of this Order, the term "Information" includes documents, testimony, written discovery, deposition transcripts and other communications of any kind (whether oral, written or otherwise), and the contents or substance thereof. Anything that discloses the contents or substance of Confidential Information shall be deemed Confidential Information for purposes of this Order.

2. What Information May Be Designated Confidential. Information may be designated as Confidential Information if the party or nonparty making the designation believes or asserts in good faith that such material:

(a) constitutes a trade secret, proprietary information or other sensitive or confidential business records, data, research, development or commercial information;

(b) private, financial or other sensitive information, including but not limited to private information protected by statute, rule, regulation or other rights of privacy; or

(c) is otherwise properly subject to a confidentiality order under Rule 26(c) of the Federal Rules of Civil Procedure.

3. Who May Designate Information Confidential. Information produced pursuant to the Subpoena, including but not limited to documents, interrogatory answers and deposition testimony, may be designated as Confidential Information, in whole or in part, by: (i) the party or nonparty producing the information, or (ii) any party to this Action or the related action, *Jonathan E. Perlman v. PNC Bank, N.A.*, 19-CIV-61390-RS (the "Related Action") asserting an interest in maintaining the confidentiality of such information.

4. No Restriction on Party's or Nonparty's Own Confidential Information. The provisions of this Order requiring confidential treatment of Confidential Information or restricting the use of Confidential Information shall not be construed to prevent any person subject to this Protective Order from using or disclosing its own Confidential Information in the Action or otherwise. This provision does not prevent a party from arguing that such disclosure would constitute waiver of confidentiality, depending on the circumstance of disclosure.

5. Manner in Which Information May Be Designated Confidential. A party or nonparty may designate information as Confidential Information by giving notice in writing or on the record of a deposition or court proceeding, to all parties to this Action or the Related Action who received the information that the information is being designated as Confidential Information. In addition, a person producing a document may designate the document and the contents thereof as Confidential Information by producing the document marked with the word "Confidential". The failure to mark a document as "Confidential" at the time of production shall not constitute a waiver of the right to designate the document as Confidential Information at a later time.

A party or non-party seeking to designate information as Confidential Information should do so:

(a) at the time any such information or a copy of any such document is provided to the requesting party;

(b) prior to or at the time any such document or information is produced for inspection;

(c) in the case of testimony, at the time the testimony is given by so stating on the record or, within 15 days after the transcript of such testimony is made available to the designating party by providing to all counsel written notice of those portions of the transcript so designated; the Court Reporter shall promptly conform the original transcript of such testimony by stamping the word CONFIDENTIAL on each page so designated; all counsel shall conform their copies of the transcript in accordance with the designation; the portions so designated shall not be utilized or disclosed by any other party, its agents, or its employees except in accordance with the terms of this Order; regardless of whether any designations are made by counsel at the deposition or during the time period within which a party may make a designation, all parties will treat the transcript as having been designated CONFIDENTIAL for fifteen (15) days from receipt of such transcript; or

(d) in the case of information presented in a pleading or memorandum, at the time of filing.

6. Withdrawal of Designation or Consent to Disclosure or Use. A party or nonparty designating information as Confidential Information may withdraw such designation or may consent to the disclosure or use of such information beyond the terms of this Order, without prejudice to any designation by any other party or nonparty, by so notifying all parties to this Action or the Related Action in writing or on the record of a deposition or court proceeding.

7. Restriction on Disclosure of Confidential Information. Any person receiving Confidential Information as a result of discovery under the Subpoena shall, pursuant to the Federal Rules of Civil Procedure, have a duty to preserve its confidentiality. Confidential Information shall not be disclosed to anyone other than:

(a) the parties' counsel;

(b) non-party employees of such counsel assigned to and necessary to assist such counsel in this Action or the Related Action;

(c) the parties;

(d) the officers, directors, employees, principals, or partners of the party that designated the information as Confidential Information;

(e) non-party expert witnesses, to the extent necessary to assist a party's counsel in this Action or the Related Action;

(f) court reporters, to the extent necessary for the purposes of this Action or the Related Action; and

(g) court personnel to the extent necessary for the purposes of this Action or the Related Action.

Without limiting the generality of these restrictions on disclosure, Confidential Information shall not be provided to any person unless that person is one of the persons to whom disclosure is expressly authorized under subparagraphs (a) through (g) of this paragraph. Confidential Information shall be used solely for the prosecution or defense of claims between the parties in this lawsuit or the Related Action, and shall not be used for any other purpose (including but not limited to commercial, business, competitive or other purposes), for any reason whatsoever, without the prior written consent of the designating party or nonparty (and, if required, the consent of a regulatory agency or other authority), and shall be disclosed to no one except those listed herein in paragraph 7. Notwithstanding the foregoing, the Receiver may use Confidential Information to the extent necessary and appropriate under the Court's Preliminary Injunction Order [DE 21] and Default Final Judgment and Order for Permanent Relief and Monetary Judgment Against the Corporate Defendants [DE 293] entered in this Action, including by sharing Confidential Information with counsel for the Federal Trade Commission and the State of Florida

Attorney General's office. Except as provided herein, the Receiver shall maintain the confidentiality of the Confidential Information in accordance with this Order.

8. Notification of Restriction on Use and Disclosure. Before any person listed in paragraph 7(b), (c), and (e) through (g) is given access to Confidential Information the attorney supplying the Confidential Information shall provide the recipient a copy of this Order and notify the recipient that their receipt of the Confidential Information is subject to the terms of this Order. Every such person shall be subject to such terms, including but not limited to the requirement that such Confidential Information may not be disclosed to any person other than as authorized by this Order.

9. Notice of Intent to Use Confidential Information in Depositions or Hearings, at Trial or in Court Filings. Counsel shall give notice in accordance with this paragraph if counsel intends to file with the Court any transcript, pleading, affidavit, memorandum, exhibit or other document containing or constituting Confidential Information. Such notice shall be given to counsel for each party and to counsel for any nonparty that has designated the information as Confidential Information pursuant to this Order. The notice shall be given reasonably in advance of such inquiry, use or filing of Confidential Information, to enable the person receiving such notice to assert its rights under this Order, to move the Court for further relief, or to waive compliance with this Order. The confidentiality of any Confidential Information in depositions shall be maintained as specified in paragraph 10 hereof. Any Confidential Information filed with the Court shall be filed under seal as specified in paragraph 11 hereof. Any party, and any nonparty producing Confidential Information, may move the Court to establish such further safeguards as may be necessary to protect against disclosure of Confidential Information.

10. Confidential Information in Depositions. If counsel for any party or counsel for any nonparty witness determines that testimony given or to be given during a deposition in this Action or the Related Action is Confidential Information, such counsel may request that all persons, other than counsel, the court reporter, the witness and other persons entitled to receive Confidential Information pursuant to Paragraph 7 hereof, leave the deposition room during the confidential portion of the deposition. Further, each transcript of a deposition shall be treated as Confidential Information until fifteen (15) days after such transcript is actually received by counsel for each party and for the witness, in order to permit such counsel to designate portions of the transcript and exhibits as Confidential Information. Upon such timely designation, the Court Reporter shall promptly conform the original transcript of such testimony by stamping the word CONFIDENTIAL on each page so designated, all counsel shall conform their copies of the transcript in accordance with the designation, and the portions so designated shall not be utilized or disclosed by any other party, its agents, or its employees except in accordance with the terms of this Order.

11. Sealing of Confidential Information in Court Filings. Before filing any item designated as containing Confidential Information, the filing party shall file a motion under the Court's Local Rules and procedures to file the item under seal. If the Court grants the motion then the filing party shall file the item under seal. If the Court denies the motion then it shall be treated as a determination under this Order that the item is not confidential. The designating party may seek review of a determination of non-confidentiality in accordance with applicable law. The filing party has no obligation to seek such review.

12. Notice of Demand for Confidential Information. In the event that any party or other person who has received Confidential Information under this Order is requested or required to disclose any Confidential Information, whether by subpoena, interrogatory, request for production, request for admission, civil investigative demand, oral question in a deposition or hearing, or any other procedure or process (each of which is referred to herein as a "Demand"), such person shall promptly notify counsel for all parties and for any nonparty who designated the material as Confidential Information pursuant to this Order. Such notice shall be given promptly, and in no event more than two (2) business days after receipt of the Demand, to enable the notified person to seek a protective order or other appropriate remedy or to waive compliance with the provisions of this Order. In the event that a protective order is not obtained, the person receiving the Demand shall not disclose any Confidential Information, except to the extent required by law.

13. Information that is not Confidential. Notwithstanding anything to the contrary contained herein, Confidential Information does not include information: (i) that is or becomes generally available to the public other than as a result of a disclosure by a party, person, or entity in breach of this Order; or (ii) that is or becomes available to the receiving party on a non-confidential basis from a source other than the other parties or a producing nonparty or the Related Action, provided that such source is not bound by a confidentiality agreement with or other contractual, legal, or fiduciary obligation of confidentiality to any other party or producing nonparty in this Action or the Related Action with respect to such information.

14. Disclosure of Confidential Information. If any Confidential Information is disclosed to any person or entity other than in the manner authorized by this Order, the person or entity

responsible for the disclosure shall, upon discovery of the disclosure, promptly inform the party or person who designated the disclosed information Confidential of all facts pertinent thereto which, after due diligence and prompt investigation, are known to the party responsible for the disclosure, including the name, address and employer of the person to whom the disclosure was made and the date of disclosure, and shall make reasonable efforts to prevent disclosure by each unauthorized person who receives such information and to retrieve from that unauthorized person all copies of documents containing that Confidential Information.

15. Challenge to Designation of Confidentiality. Nothing in this Order shall limit any of the parties from challenging designations of confidentiality under this Order, or from requesting the Court to provide further or additional protections of confidentiality, or from agreeing between themselves to any modification of this Order subject to approval of the Court. If any Party objects to the designation of any material as "CONFIDENTIAL," the parties will meet and confer in an effort to resolve the dispute. If the designating and objecting parties are unable to resolve the dispute, then, within 10 days of the objection, the designating party shall apply to the Court for a determination in accordance with Florida law and the standards set forth in this Order. A failure of a party to challenge a designation of confidentiality when made shall not be a waiver of that party's right to later assert that the information actually is not confidential or entitled to the protection of this Order. The contested information and documents shall retain their protected confidential status pending resolution of the dispute.

16. No Waiver of Objections to Admissibility. This Order and the definitions herein shall not constitute a waiver by the parties of any objection which might be raised as to the production or use of documents and information, including the admissibility of any documents or

information into evidence in this Action or the Related Action and each party reserves such rights, privileges and objections. Moreover, this Order does not constitute an agreement to produce any documents, including but not limited to documents which a party is prohibited from producing by law or regulation.

17. Survival of Order: Retention of Jurisdiction. The provisions of this Order shall survive the termination of this Action. This Court retains jurisdiction following the termination of this Action for purposes of any proceedings for the enforcement or modification of this Order. The parties agree that injunctive relief is the only appropriate way to remedy a violation of this Order and that no monetary or different relief is available under this Order.

18. Disposition of Confidential Information. Unless the Court orders otherwise, at the conclusion of this Action and the Related Action, or such earlier time as the parties to the Related Action may agree, all Confidential Information in the possession of the parties or their counsel shall be returned to the person who produced such information or destroyed at the option of the person who produced such information. All persons who have received Confidential Information under this Order shall certify in writing, within 30 days of the conclusion of this Action, that all Confidential Information has in fact been returned or destroyed.

19. Right to Seek Modification or Further Order. Nothing herein shall preclude any party from seeking from the Court (a) a modification of this Order, subject to the procedures set forth in paragraph 15 hereof, or (b) a further protective order.

20. Paragraph Titles. The paragraph titles in this Order are for convenience of reference only and shall not in any way restrict or alter the meaning of any provision hereof.

Dated: _____, 2019.

**IT IS SO ORDERED:**

_____
FEDERICO A. MORENO
UNITED STATES DISTRICT JUDGE

# EXHIBIT

# B

**UNITED STATES DISTRICT COURT**
**SOUTHERN DISTRICT OF FLORIDA**

**Case No. 17-60907-Civ-Moreno/Seltzer**

FEDERAL TRADE COMMISSION, *et al.*

Plaintiffs,

v.

JEREMY LEE MARCUS, *et al.*,

Defendants.

---

**STIPULATED CONFIDENTIALITY AGREEMENT AND [PROPOSED] PROTECTIVE ORDER**

WHEREAS, Jonathan E. Perlman, the Court-appointed Receiver ("Receiver") of the Receivership Entities in the above-captioned case, served PNC Bank, N.A. ("PNC") with a subpoena *duces tecum* on May 1, 2018 seeking production of documents (the "Subpoena"); and

WHEREAS, on April 2, 2019, the Receiver moved to compel production of documents responsive to the Subpoena (D.I. 357); and

WHEREAS, on April 29, 2019, PNC opposed the Receiver's motion to compel (D.I. 363); and

WHEREAS, on June 11, 2019 this Court denied the Receiver's motion to compel (D.I. 380); and

WHEREAS, the Receiver and PNC have nevertheless conferred and agreed upon production of certain documents responsive to the Subpoena; and

WHEREAS, the documents to be produced pursuant to such agreement contain financial and other sensitive information which may be confidential; and

WHEREAS, the Receiver and PNC stipulate that good cause exists for the entry of this Protective Order (the "Order").

NOW THEREFORE, the Receiver and PNC (each a "party" and together, the "parties") hereby stipulate and agree that, upon entry by the Court pursuant to Rule 26(c) of the Federal Rules of Civil Procedure, the following Order shall govern the disclosure of confidential information from PNC to the Receiver in the above-referenced case, *Federal Trade Commission, et al., v. Jeremy Lee Marcus, et al.* 17-60907-Moreno/Seltzer, currently pending in the United States District Court for the Southern District of Florida (the "Action").

1. Scope of Order. All information disclosed pursuant to the Subpoena is subject to this Order and shall be deemed Confidential Information to the extent that it is designated as Confidential Information pursuant to this Order. Confidential Information shall not be used or disclosed to anyone except as provided in this Order. For the purposes of this Order, the term "Information" includes documents, testimony, written discovery, deposition transcripts and other communications of any kind (whether oral, written or otherwise), and the contents or substance thereof. Anything that discloses the contents or substance of Confidential Information shall be deemed Confidential Information for purposes of this Order.

2. What Information May Be Designated Confidential. Information may be designated as Confidential Information if the party or nonparty making the designation believes or asserts in good faith that such material:

(a) constitutes a trade secret, proprietary information or other sensitive or confidential business records, data, research, development or commercial information;

(b) private, financial or other sensitive information, including but not limited to private information protected by statute, rule, regulation or other rights of privacy; or

(c) is otherwise properly subject to a confidentiality order under Rule 26(c) of the Federal Rules of Civil Procedure.

3. Who May Designate Information Confidential. Information produced pursuant to the Subpoena, including but not limited to documents, interrogatory answers and deposition testimony, may be designated as Confidential Information, in whole or in part, by: (i) the party or nonparty producing the information, or (ii) any party to this Action or the related action, *Jonathan E. Perlman v. PNC Bank, N.A.*, 19-CIV-61390-RS (the "Related Action") asserting an interest in maintaining the confidentiality of such information.

4. No Restriction on Party's or Nonparty's Own Confidential Information. The provisions of this Order requiring confidential treatment of Confidential Information or restricting the use of Confidential Information shall not be construed to prevent any person subject to this Protective Order from using or disclosing its own Confidential Information in the Action or otherwise. This provision does not prevent a party from arguing that such disclosure would constitute waiver of confidentiality, depending on the circumstance of disclosure.

5. Manner in Which Information May Be Designated Confidential. A party or nonparty may designate information as Confidential Information by giving notice in writing or on the record of a deposition or court proceeding, to all parties to this Action or the Related Action who received the information that the information is being designated as Confidential Information. In addition, a person producing a document may designate the document and the contents thereof as Confidential Information by producing the document marked with the word "Confidential". The failure to mark

a document as "Confidential" at the time of production shall not constitute a waiver of the right to designate the document as Confidential Information at a later time.

A party or non-party seeking to designate information as Confidential Information should do so:

(a) at the time any such information or a copy of any such document is provided to the requesting party;

(b) prior to or at the time any such document or information is produced for inspection;

(c) in the case of testimony, at the time the testimony is given by so stating on the record or, within 15 days after the transcript of such testimony is made available to the designating party by providing to all counsel written notice of those portions of the transcript so designated; the Court Reporter shall promptly conform the original transcript of such testimony by stamping the word CONFIDENTIAL on each page so designated; all counsel shall conform their copies of the transcript in accordance with the designation; the portions so designated shall not be utilized or disclosed by any other party, its agents, or its employees except in accordance with the terms of this Order; regardless of whether any designations are made by counsel at the deposition or during the time period within which a party may make a designation, all parties will treat the transcript as having been designated CONFIDENTIAL for fifteen (15) days from receipt of such transcript; or

(d) in the case of information presented in a pleading or memorandum, at the time of filing.

6. Withdrawal of Designation or Consent to Disclosure or Use. A party or nonparty designating information as Confidential Information may withdraw such designation or may consent to the disclosure or use of such information beyond the terms of this Order, without prejudice to any designation by any other party or nonparty, by so notifying all parties to this Action or the Related Action in writing or on the record of a deposition or court proceeding.

7. Restriction on Disclosure of Confidential Information. Any person receiving Confidential Information as a result of discovery under the Subpoena shall, pursuant to the Federal Rules of Civil Procedure, have a duty to preserve its confidentiality. Confidential Information shall not be disclosed to anyone other than:

(a) the parties' counsel;

(b) non-party employees of such counsel assigned to and necessary to assist such counsel in this Action or the Related Action;

(c) the parties;

(d) the officers, directors, employees, principals, or partners of the party that designated the information as Confidential Information;

(e) non-party expert witnesses, to the extent necessary to assist a party's counsel in this Action or the Related Action;

(f) court reporters, to the extent necessary for the purposes of this Action or the Related Action; and

(g) court personnel to the extent necessary for the purposes of this Action or the Related Action.

Without limiting the generality of these restrictions on disclosure, Confidential Information shall not be provided to any person unless that person is one of the persons to whom disclosure is expressly authorized under subparagraphs (a) through (g) of this paragraph. Confidential Information shall be used solely for the prosecution or defense of claims between the parties in this lawsuit or the Related Action, and shall not be used for any other purpose (including but not limited to commercial, business, competitive or other purposes), for any reason whatsoever, without the prior written consent of the designating party or nonparty (and, if required, the consent of a regulatory agency or other authority), and shall be disclosed to no one except those listed herein in paragraph 7. Notwithstanding the foregoing, the Receiver may use Confidential

Information to the extent necessary and appropriate under the Court's Preliminary Injunction Order [DE 21] and Default Final Judgment and Order for Permanent Relief and Monetary Judgment Against the Corporate Defendants [DE 293] entered in this Action, including by sharing Confidential Information with counsel for the Federal Trade Commission and the State of Florida Attorney General's office. Except as provided herein, the Receiver shall maintain the confidentiality of the Confidential Information in accordance with this Order.

8. Notification of Restriction on Use and Disclosure. Before any person listed in paragraph 7(b), (c), and (e) through (g) is given access to Confidential Information the attorney supplying the Confidential Information shall provide the recipient a copy of this Order and notify the recipient that their receipt of the Confidential Information is subject to the terms of this Order. Every such person shall be subject to such terms, including but not limited to the requirement that such Confidential Information may not be disclosed to any person other than as authorized by this Order.

9. Notice of Intent to Use Confidential Information in Depositions or Hearings, at Trial or in Court Filings. Counsel shall give notice in accordance with this paragraph if counsel intends to file with the Court any transcript, pleading, affidavit, memorandum, exhibit or other document containing or constituting Confidential Information. Such notice shall be given to counsel for each party and to counsel for any nonparty that has designated the information as Confidential Information pursuant to this Order. The notice shall be given reasonably in advance of such inquiry, use or filing of Confidential Information, to enable the person receiving such notice to assert its rights under this Order, to move the Court for further relief, or to waive compliance with this Order. The confidentiality of any Confidential Information in depositions

shall be maintained as specified in paragraph 10 hereof. Any Confidential Information filed with the Court shall be filed under seal as specified in paragraph 11 hereof. Any party, and any nonparty producing Confidential Information, may move the Court to establish such further safeguards as may be necessary to protect against disclosure of Confidential Information.

10. Confidential Information in Depositions. If counsel for any party or counsel for any nonparty witness determines that testimony given or to be given during a deposition in this Action or the Related Action is Confidential Information, such counsel may request that all persons, other than counsel, the court reporter, the witness and other persons entitled to receive Confidential Information pursuant to Paragraph 7 hereof, leave the deposition room during the confidential portion of the deposition. Further, each transcript of a deposition shall be treated as Confidential Information until fifteen (15) days after such transcript is actually received by counsel for each party and for the witness, in order to permit such counsel to designate portions of the transcript and exhibits as Confidential Information. Upon such timely designation, the Court Reporter shall promptly conform the original transcript of such testimony by stamping the word CONFIDENTIAL on each page so designated, all counsel shall conform their copies of the transcript in accordance with the designation, and the portions so designated shall not be utilized or disclosed by any other party, its agents, or its employees except in accordance with the terms of this Order.

11. Sealing of Confidential Information in Court Filings. Before filing any item designated as containing Confidential Information, the filing party shall file a motion under the Court's Local Rules and procedures to file the item under seal. If the Court grants the motion then the filing party shall file the item under seal. If the Court denies the motion then it shall be treated

as a determination under this Order that the item is not confidential. The designating party may seek review of a determination of non-confidentiality in accordance with applicable law. The filing party has no obligation to seek such review.

12. Notice of Demand for Confidential Information. In the event that any party or other person who has received Confidential Information under this Order is requested or required to disclose any Confidential Information, whether by subpoena, interrogatory, request for production, request for admission, civil investigative demand, oral question in a deposition or hearing, or any other procedure or process (each of which is referred to herein as a "Demand"), such person shall promptly notify counsel for all parties and for any nonparty who designated the material as Confidential Information pursuant to this Order. Such notice shall be given promptly, and in no event more than two (2) business days after receipt of the Demand, to enable the notified person to seek a protective order or other appropriate remedy or to waive compliance with the provisions of this Order. In the event that a protective order is not obtained, the person receiving the Demand shall not disclose any Confidential Information, except to the extent required by law.

13. Information that is not Confidential. Notwithstanding anything to the contrary contained herein, Confidential Information does not include information: (i) that is or becomes generally available to the public other than as a result of a disclosure by a party, person, or entity in breach of this Order; or (ii) that is or becomes available to the receiving party on a non-confidential basis from a source other than the other parties or a producing nonparty or the Related Action, provided that such source is not bound by a confidentiality agreement with or

other contractual, legal, or fiduciary obligation of confidentiality to any other party or producing nonparty in this Action or the Related Action with respect to such information.

14. Disclosure of Confidential Information. If any Confidential Information is disclosed to any person or entity other than in the manner authorized by this Order, the person or entity responsible for the disclosure shall, upon discovery of the disclosure, promptly inform the party or person who designated the disclosed information Confidential of all facts pertinent thereto which, after due diligence and prompt investigation, are known to the party responsible for the disclosure, including the name, address and employer of the person to whom the disclosure was made and the date of disclosure, and shall make reasonable efforts to prevent disclosure by each unauthorized person who receives such information and to retrieve from that unauthorized person all copies of documents containing that Confidential Information.

15. Challenge to Designation of Confidentiality. Nothing in this Order shall limit any of the parties from challenging designations of confidentiality under this Order, or from requesting the Court to provide further or additional protections of confidentiality, or from agreeing between themselves to any modification of this Order subject to approval of the Court. If any Party objects to the designation of any material as "CONFIDENTIAL," the parties will meet and confer in an effort to resolve the dispute. If the designating and objecting parties are unable to resolve the dispute, then, within 10 days of the objection, the designating party shall apply to the Court for a determination in accordance with Florida law and the standards set forth in this Order. A failure of a party to challenge a designation of confidentiality when made shall not be a waiver of that party's right to later assert that the information actually is not confidential or entitled to the

protection of this Order. The contested information and documents shall retain their protected confidential status pending resolution of the dispute.

16. No Waiver of Objections to Admissibility. This Order and the definitions herein shall not constitute a waiver by the parties of any objection which might be raised as to the production or use of documents and information, including the admissibility of any documents or information into evidence in this Action or the Related Action and each party reserves such rights, privileges and objections. Moreover, this Order does not constitute an agreement to produce any documents, including but not limited to documents which a party is prohibited from producing by law or regulation.

17. Survival of Order: Retention of Jurisdiction. The provisions of this Order shall survive the termination of this Action. This Court retains jurisdiction following the termination of this Action for purposes of any proceedings for the enforcement or modification of this Order. The parties agree that injunctive relief is the only appropriate way to remedy a violation of this Order and that no monetary or different relief is available under this Order.

18. Disposition of Confidential Information. Unless the Court orders otherwise, at the conclusion of this Action and the Related Action, or such earlier time as the parties to the Related Action may agree, all Confidential Information in the possession of the parties or their counsel shall be returned to the person who produced such information or destroyed at the option of the person who produced such information. All persons who have received Confidential Information under this Order shall certify in writing, within 30 days of the conclusion of this Action, that all Confidential Information has in fact been returned or destroyed.

19. Right to Seek Modification or Further Order. Nothing herein shall preclude any party from seeking from the Court (a) a modification of this Order, subject to the procedures set forth in paragraph 15 hereof, or (b) a further protective order.

20. Paragraph Titles. The paragraph titles in this Order are for convenience of reference only and shall not in any way restrict or alter the meaning of any provision hereof.

Dated: _____, 2019

**IT IS SO ORDERED:**

_____
FEDERICO A. MORENO
UNITED STATES DISTRICT JUDGE

STIPULATED AND AGREED:

GENEVESE JOBLOVE

/s/ *William Barry Blum*_____
William Barry Blum
Michael A. Freidman
Gregory Matthew Garno
100 SE 2nd Street, Suite 4400
Tampa, FL 33131
(305-349-2339)

*Attorneys for Jonathan E. Perlman as Court Appointed Receiver*

BALLARD SPAHR LLP

/s/ *Peter D. Hardy*_____
Peter D. Hardy (admitted *Pro Hac Vice*)
Melanie J. Vartabedian (admitted *Pro Hac Vice*)
Diana M. Joskowicz (admitted *Pro Hac Vice*)
Mark S. Kokanovich (admitted *Pro Hac Vice*)
1735 Market Street, 51st Floor
Philadelphia, PA 19103
Telephone: (305) 374-7771

HOMER BONNER JACOBS

/s/ *Peter W. Homer*_____
Peter W. Homer
Florida Bar No. 291250
1200 Four Seasons Tower, 1441 Brickell Avenue
Miami, Florida 33131
phomer@homerbonner.com

*Attorneys for Non-Party PNC Bank NA*