IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

WILLIAM GRECIA, Plaintiff, v. MCDONALD'S CORPORATION, Defendant.	Case No.

COMPLAINT FOR PATENT INFRINGEMENT

William Grecia brings this claim of patent infringement against McDonald's Corporation ("McDonald's").

The Parties

1. William Grecia is an individual who resides in Downingtown, Pennsylvania.

2. McDonald's is a Delaware corporation with its principal place of business in Illinois.

Jurisdiction And Venue

3. This is an action for patent infringement arising under the patent laws of the United States, Title 35 of the United States Code.

4. This Court has subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a).

5. This Court has personal jurisdiction over McDonald's. McDonald's maintains corporate offices in this judicial district. McDonald's has done and does continuous and systematic business in Illinois, and this patent-infringement action arises directly from McDonald's continuous and systematic activity in this District. In short, this Court's exercise of

jurisdiction over McDonald's would be consistent with the Illinois long-arm statute, 735 ILCS § 5/2-209, and traditional notions of fair play and substantial justice.

6. Venue is proper in this district under 28 U.S.C. §§ 1391(b)(1)-(2) and 1400(b) because McDonald's resides in, and a substantial part of the events giving rise to these claims occurred and are occurring, in this judicial district.

Count 1: Infringement Of U.S. Patent No. 8,533,860

7. Mr. Grecia re-alleges and incorporates by reference the above paragraphs of this Complaint as though fully set forth in this Paragraph 7.

8. Mr. Grecia is the sole inventor and owner of U.S. Patent No. 8,533,860 (the "'860 patent") (attached hereto as "Exhibit A").

9. McDonald's has infringed and continues to infringe the system claims of the '860 patent, claims 9 and 10, through its use of the tokenization systems of Visa Inc. (hereinafter, "Visa"), American Express Company (hereinafter, "AMEX"), MasterCard Incorporated (hereinafter, "MasterCard"), and Discover Financial Services (hereinafter, "Discover").

10. Claim 9 is a "system for authorizing access to digital content using a worldwide cloud system infrastructure . . . ." (Ex. A, 15:45-46.) As set forth below, McDonald's uses the system of claim 9 each time that McDonald's puts the Visa tokenization system into service as follows:

a. Claim 9 includes "a first receipt module, the first receipt module receiving a digital content access request from at least one communications console . . . the access request being a read or write request of metadata of the digital content . . . the request comprising a verification token provided by a user corresponding to the digital content, wherein the verification token is one or more of . . . a rights token . . . ." (Ex. A, 15:56-16:2.)

McDonald's pays Visa fees in exchange for McDonald's' ability to process transactions that put the Visa tokenization system into service. When a McDonald's customer purchases a hamburger at McDonald's with his Visa card, a VisaNet server receives the customer's primary account number ("PAN") assigned to the credit card. Receipt of the PAN is a request to write a token to the Visa token vault. The token will thereafter be associated with the customer's PAN. In this way, the token is "metadata"—i.e., the data (token) about the data (PAN).

b. Claim 9 has "an authentication module, the authentication module authenticating the verification token . . . ." (Ex. A, 16:4-5.) After Visa receives the McDonald's customer's PAN, Visa uses the authentication module to authenticate the PAN with the issuer of the Visa card.

c. Claim 9 also has "a connection module, the connection module establishing a connection with the at least one communications console, wherein the communications console is a combination of a graphic user interface (GUI) and an Application Programmable Interface (API) wherein the API is related to a verified web service, the web service capable of facilitating a two way data exchange session to complete a verification process wherein the data exchange session comprises at least one identification reference . . . ." (Ex. A, 16:6-14.) After Visa has authenticated the McDonald's customer's PAN, Visa uses the connection module to establish a connection between the Visa payment processor and Visa's token service provider. This API communication is possible

because Visa has been issued and assigned a "Token Requestor ID" per the EMVCo Tokenization Specification.

d. In claim 9, there is "a request module, the request module requesting the at least one identification reference from the at least one communications console, wherein the identification reference comprises one or more of a . . . letter, number, rights token . . . ." (Ex. A, 16:15-19.) The Visa payment processor uses the API connection with the token service provider to request the token associated with the customer's PAN.

e. Claim 9 includes "a secondary receipt module, the secondary receipt module receiving the at least one identification reference from the at least one communications console . . . ." (Ex. A, 16:23-25.) The token is received by the Visa payment processor from the token service provider.

f. Claim 9 has "a branding module, the branding module writing at least one of the verification token or the identification reference into the metadata." (Ex. A, 16:26-28.) Visa writes the token to the token vault, associating the token to the PAN for later cross-referencing upon subsequent hamburger purchases at this McDonald's.

11. As set forth below, McDonald's uses the system of claim 9 each time that McDonald's puts the AMEX tokenization system into service as follows:

a. Claim 9 includes "a first receipt module, the first receipt module receiving a digital content access request from at least one communications console . . . the access request being a read or write request of metadata of the digital content . . . the request comprising a verification token provided by a user corresponding to the digital content, wherein the verification token

is one or more of . . . a rights token . . . .” (Ex. A, 15:56-16:2.) McDonald’s pays AMEX fees in exchange for McDonald’s’ ability to process transactions that put the AMEX tokenization system into service. When a McDonald’s customer purchases a hamburger at McDonald’s with his AMEX card, an AMEX Global Network server receives the customer’s PAN assigned to the credit card. Receipt of the PAN is a request to write a token to the AMEX token vault. The token will thereafter be associated with the customer’s PAN. In this way, the token is “metadata”—i.e., the data (token) about the data (PAN).

b. Claim 9 has “an authentication module, the authentication module authenticating the verification token . . . .” (Ex. A, 16:4-5.) After AMEX receives the McDonald’s customer’s PAN, AMEX uses the authentication module to authenticate the PAN with the issuer of the AMEX card.

c. Claim 9 also has “a connection module, the connection module establishing a connection with the at least one communications console, wherein the communications console is a combination of a graphic user interface (GUI) and an Application Programmable Interface (API) wherein the API is related to a verified web service, the web service capable of facilitating a two way data exchange session to complete a verification process wherein the data exchange session comprises at least one identification reference . . . .” (Ex. A, 16:6-14.) After AMEX has authenticated the McDonald’s customer’s PAN, AMEX uses the connection module to establish a connection between the AMEX payment processor and AMEX’s token service provider. This API communication

is possible because AMEX has been issued and assigned a "Token Requestor ID" per the EMVCo Tokenization Specification.

d. In claim 9, there is "a request module, the request module requesting the at least one identification reference from the at least one communications console, wherein the identification reference comprises one or more of a . . . letter, number, rights token . . . ." (Ex. A, 16:15-19.) The AMEX payment processor uses the API connection with the token service provider to request the token associated with the customer's PAN.

e. Claim 9 includes "a secondary receipt module, the secondary receipt module receiving the at least one identification reference from the at least one communications console . . . ." (Ex. A, 16:23-25.) The token is received by the AMEX payment processor from the token service provider.

f. Claim 9 has "a branding module, the branding module writing at least one of the verification token or the identification reference into the metadata." (Ex. A, 16:26-28.) AMEX writes the token to the token vault, associating the token to the PAN for later cross-referencing upon subsequent hamburger purchases at this McDonald's.

12. As set forth below, McDonald's uses the system of claim 9 each time that McDonald's puts the MasterCard tokenization system into service as follows:

a. Claim 9 includes "a first receipt module, the first receipt module receiving a digital content access request from at least one communications console . . . the access request being a read or write request of metadata of the digital content . . . the request comprising a verification token provided by

a user corresponding to the digital content, wherein the verification token is one or more of . . . a rights token . . . .” (Ex. A, 15:56-16:2.) McDonald’s pays MasterCard fees in exchange for McDonald’s’ ability to process transactions that put the MasterCard tokenization system into service. When a McDonald’s customer purchases a hamburger at McDonald’s with his card, a BankNet server receives the customer’s PAN assigned to the credit card. Receipt of the PAN is a request to write a token to the MasterCard token vault. The token will thereafter be associated with the customer’s PAN. In this way, the token is “metadata”—i.e., the data (token) about the data (PAN).

b. Claim 9 has “an authentication module, the authentication module authenticating the verification token . . . .” (Ex. A, 16:4-5.) After MasterCard receives the McDonald’s customer’s PAN, MasterCard uses the authentication module to authenticate the PAN with the issuer of this credit card.

c. Claim 9 also has “a connection module, the connection module establishing a connection with the at least one communications console, wherein the communications console is a combination of a graphic user interface (GUI) and an Application Programmable Interface (API) wherein the API is related to a verified web service, the web service capable of facilitating a two way data exchange session to complete a verification process wherein the data exchange session comprises at least one identification reference . . . .” (Ex. A, 16:6-14.) After MasterCard has authenticated the McDonald’s customer’s PAN, MasterCard uses the

connection module to establish a connection between the MasterCard payment processor and MasterCard's token service provider. This API communication is possible because MasterCard has been issued and assigned a "Token Requestor ID" per the EMVCo Tokenization Specification.

d. In claim 9, there is "a request module, the request module requesting the at least one identification reference from the at least one communications console, wherein the identification reference comprises one or more of a . . . letter, number, rights token . . . ." (Ex. A, 16:15-19.) The MasterCard payment processor uses the API connection with the token service provider to request the token associated with the customer's PAN.

e. Claim 9 includes "a secondary receipt module, the secondary receipt module receiving the at least one identification reference from the at least one communications console . . . ." (Ex. A, 16:23-25.) The token is received by the MasterCard payment processor from the token service provider.

f. Claim 9 has "a branding module, the branding module writing at least one of the verification token or the identification reference into the metadata." (Ex. A, 16:26-28.) MasterCard writes the token to the token vault, associating the token to the PAN for later cross-referencing upon subsequent hamburger purchases at this McDonald's.

13. As set forth below, McDonald's uses the system of claim 9 each time that McDonald's puts the Discover tokenization system into service as follows:

a. Claim 9 includes "a first receipt module, the first receipt module receiving a digital content access request from at least one communications console . . . the access request being a read or write request of metadata of the digital content . . . the request comprising a verification token provided by a user corresponding to the digital content, wherein the verification token is one or more of . . . a rights token . . . ." (Ex. A, 15:56-16:2.) McDonald's pays Discover fees in exchange for McDonald's' ability to process transactions that put the Discover tokenization system into service. When a McDonald's customer purchases a hamburger at McDonald's with his Discover card, Discover receives the customer's PAN assigned to the credit card. Receipt of the PAN is a request to write a token to the Discover token vault. The token will thereafter be associated with the customer's PAN. In this way, the token is "metadata"—i.e., the data (token) about the data (PAN).

b. Claim 9 has "an authentication module, the authentication module authenticating the verification token . . . ." (Ex. A, 16:4-5.) After Discover receives the McDonald's customer's PAN, Discover uses the authentication module to authenticate the PAN with the issuer of the Discover card.

c. Claim 9 also has "a connection module, the connection module establishing a connection with the at least one communications console, wherein the communications console is a combination of a graphic user interface (GUI) and an Application Programmable Interface (API) wherein the API is related to a verified web service, the web service capable of

facilitating a two way data exchange session to complete a verification process wherein the data exchange session comprises at least one identification reference . . . .” (Ex. A, 16:6-14.) After Discover has authenticated the McDonald’s customer’s PAN, Discover uses the connection module to establish a connection between the Discover payment processor and Discover’s token service provider. This API communication is possible because Discover has been issued and assigned a “Token Requestor ID” per the EMVCo Tokenization Specification.

d. In claim 9, there is “a request module, the request module requesting the at least one identification reference from the at least one communications console, wherein the identification reference comprises one or more of a . . . letter, number, rights token . . . .” (Ex. A, 16:15-19.) The Discover payment processor uses the API connection with the token service provider to request the token associated with the customer’s PAN.

e. Claim 9 includes “a secondary receipt module, the secondary receipt module receiving the at least one identification reference from the at least one communications console . . . .” (Ex. A, 16:23-25.) The token is received by the Discover payment processor from the token service provider.

f. Claim 9 has “a branding module, the branding module writing at least one of the verification token or the identification reference into the metadata.” (Ex. A, 16:26-28.) Discover writes the token to the token vault, associating the token to the PAN for later cross-referencing upon subsequent hamburger purchases at this McDonald’s.

Count 2: Infringement Of U.S. Patent No. 8,402,555

14. Mr. Grecia re-alleges and incorporates by reference the above paragraphs of this Complaint as though fully set forth in this Paragraph 14.

15. Mr. Grecia is the sole inventor and owner of U.S. Patent No. 8,402,555 (the "'555 patent") (attached hereto as "Exhibit B").

16. McDonald's has infringed and continues to infringe the system claims of the '555 patent, claims 12, 13, 14, 24, 25, 26 through its use of the tokenization systems of Visa, AMEX, MasterCard, and Discover.

17. Claim 12 is a "system for monitoring access to an encrypted digital media . . . the system working as a front-end agent for access rights authorization between a plurality of data processing devices . . . ." (Ex. B, 15:65-16:2.) As set forth below, McDonald's uses the system of claim 12 each time that McDonald's puts the Visa tokenization system into service as follows:

a. Claim 12 includes "a first receipt module, the first receipt module receiving an encrypted digital media access branding request from at least one communications console . . . the branding request being a read or write request of metadata of the encrypted digital media, the request comprising a membership verification token provided by a first user, corresponding to the encrypted digital media . . . ." (Ex. B, 16:3-10.) McDonald's pays Visa fees in exchange for McDonald's' ability to process transactions that put the Visa tokenization system into service. When a McDonald's customer purchases a hamburger at McDonald's with his Visa card, a VisaNet server receives the customer's PAN assigned to the credit card. Receipt of the PAN is a request to write a token to the Visa token vault. The token will thereafter be associated with the customer's

PAN. In this way, the token is "metadata"—i.e., the data (token) about the data (PAN).

b. Claim 12 has "an authentication module, the authentication module authenticating the membership verification token, the authentication being performed in connection with a token database . . . ." (Ex. B, 16:11-14.) After Visa receives the McDonald's customer's PAN, Visa uses the authentication module to authenticate the PAN with the issuer of the Visa card.

c. Claim 12 also has "a connection module, the connection module establishing a connection with the at least one communications console, wherein the communications console is a combination of a graphic user interface (GUI) and an Application Programmable Interface (API) protocol wherein the API is related to a verified web service, the verified web service capable of facilitating a two way data exchange to complete a verification process . . . ." (Ex. B, 16:15-22.) After Visa has authenticated the McDonald's customer's PAN, Visa uses the connection module to establish a connection between the Visa payment processor and Visa's token service provider. This API communication is possible because Visa has been issued and assigned a "Token Requestor ID" per the EMVCo Tokenization Specification.

d. In claim 12, there is "a request module, the request module requesting at least one electronic identification reference from the at least one communications console wherein the electronic identification reference comprises a verified web service account identifier of the first user . . . ."

(Ex. B, 16:23-27) The Visa payment processor uses the API connection with the token servicer provider to request the token associated with the customer's PAN.

e. Claim 12 includes "a second receipt module, the second receipt module receiving the at least one electronic identification reference from the at least one communications console . . . ." (Ex. B, 16:28-30.) The token is received by the Visa payment processor from the token service provider.

f. Claim 12 has "a branding module, the branding module branding metadata of the encrypted digital media by writing the membership verification token and the electronic identification reference into the metadata." (Ex. B, 16:31-34.) Visa writes the token to the token vault, associating the token to the PAN for later cross-referencing upon subsequent hamburger purchases at this McDonald's.

18. As set forth below, McDonald's uses the system of claim 12 each time that McDonald's puts the AMEX tokenization system into service as follows:

a. Claim 12 includes "a first receipt module, the first receipt module receiving an encrypted digital media access branding request from at least one communications console . . . the branding request being a read or write request of metadata of the encrypted digital media, the request comprising a membership verification token provided by a first user, corresponding to the encrypted digital media . . . ." (Ex. B, 16:3-10.) McDonald's pays AMEX fees in exchange for McDonald's' ability to process transactions that put the AMEX tokenization system into service. When a McDonald's customer purchases a hamburger at McDonald's with

his AMEX card, an AMEX server receives the customer's PAN assigned to the credit card. Receipt of the PAN is a request to write a token to the AMEX token vault. The token will thereafter be associated with the customer's PAN. In this way, the token is "metadata"—i.e., the data (token) about the data (PAN).

b. Claim 12 has "an authentication module, the authentication module authenticating the membership verification token, the authentication being performed in connection with a token database . . . ." (Ex. B, 16:11-14.) After AMEX receives the McDonald's customer's PAN, AMEX uses the authentication module to authenticate the PAN with the issuer of the AMEX card.

c. Claim 12 also has "a connection module, the connection module establishing a connection with the at least one communications console, wherein the communications console is a combination of a graphic user interface (GUI) and an Application Programmable Interface (API) protocol wherein the API is related to a verified web service, the verified web service capable of facilitating a two way data exchange to complete a verification process . . . ." (Ex. B, 16:15-22.) After AMEX has authenticated the McDonald's customer's PAN, AMEX uses the connection module to establish a connection between the AMEX payment processor and AMEX's token service provider. This API communication is possible because AMEX has been issued and assigned a "Token Requestor ID" per the EMVCo Tokenization Specification.

d. In claim 12, there is "a request module, the request module requesting at least one electronic identification reference from the at least one communications console wherein the electronic identification reference comprises a verified web service account identifier of the first user . . . ." (Ex. B, 16:23-27) The AMEX payment processor uses the API connection with the token servicer provider to request the token associated with the customer's PAN.

e. Claim 12 includes "a second receipt module, the second receipt module receiving the at least one electronic identification reference from the at least one communications console . . . ." (Ex. B, 16:28-30.) The token is received by the AMEX payment processor from the token service provider.

f. Claim 12 has "a branding module, the branding module branding metadata of the encrypted digital media by writing the membership verification token and the electronic identification reference into the metadata." (Ex. B, 16:31-34.) AMEX writes the token to the token vault, associating the token to the PAN for later cross-referencing upon subsequent hamburger purchases at this McDonald's.

19. As set forth below, McDonald's uses the system of claim 12 each time that McDonald's puts the MasterCard tokenization system into service as follows:

a. Claim 12 includes "a first receipt module, the first receipt module receiving an encrypted digital media access branding request from at least one communications console . . . the branding request being a read or write request of metadata of the encrypted digital media, the request

comprising a membership verification token provided by a first user, corresponding to the encrypted digital media . . . .” (Ex. B, 16:3-10.) McDonald’s pays MasterCard fees in exchange for McDonald’s’ ability to process transactions that put the MasterCard tokenization system into service. When a McDonald’s customer purchases a hamburger at McDonald’s with his card, a MasterCard server receives the customer’s PAN assigned to the credit card. Receipt of the PAN is a request to write a token to the MasterCard token vault. The token will thereafter be associated with the customer’s PAN. In this way, the token is “metadata”—i.e., the data (token) about the data (PAN).

b. Claim 12 has “an authentication module, the authentication module authenticating the membership verification token, the authentication being performed in connection with a token database . . . .” (Ex. B, 16:11-14.) After MasterCard receives the McDonald’s customer’s PAN, MasterCard uses the authentication module to authenticate the PAN with the issuer of the card.

c. Claim 12 also has “a connection module, the connection module establishing a connection with the at least one communications console, wherein the communications console is a combination of a graphic user interface (GUI) and an Application Programmable Interface (API) protocol wherein the API is related to a verified web service, the verified web service capable of facilitating a two way data exchange to complete a verification process . . . .” (Ex. B, 16:15-22.) After MasterCard has authenticated the McDonald’s customer’s PAN, MasterCard uses the

connection module to establish a connection between the MasterCard payment processor and MasterCard's token service provider. This API communication is possible because MasterCard has been issued and assigned a "Token Requestor ID" per the EMVCo Tokenization Specification.

d. In claim 12, there is "a request module, the request module requesting at least one electronic identification reference from the at least one communications console wherein the electronic identification reference comprises a verified web service account identifier of the first user . . . ." (Ex. B, 16:23-27) The MasterCard payment processor uses the API connection with the token servicer provider to request the token associated with the customer's PAN.

e. Claim 12 includes "a second receipt module, the second receipt module receiving the at least one electronic identification reference from the at least one communications console . . . ." (Ex. B, 16:28-30.) The token is received by the payment processor from the token service provider.

f. Claim 12 has "a branding module, the branding module branding metadata of the encrypted digital media by writing the membership verification token and the electronic identification reference into the metadata." (Ex. B, 16:31-34.) MasterCard writes the token to the token vault, associating the token to the PAN for later cross-referencing upon subsequent hamburger purchases at this McDonald's.

20. As set forth below, McDonald's uses the system of claim 12 each time that McDonald's puts the Discover tokenization system into service as follows:

a. Claim 12 includes "a first receipt module, the first receipt module receiving an encrypted digital media access branding request from at least one communications console . . . the branding request being a read or write request of metadata of the encrypted digital media, the request comprising a membership verification token provided by a first user, corresponding to the encrypted digital media . . . ." (Ex. B, 16:3-10.) McDonald's pays Discover fees in exchange for McDonald's' ability to process transactions that put the Discover tokenization system into service. When a McDonald's customer purchases a hamburger at McDonald's with his Discover card, a Discover server receives the customer's PAN assigned to the credit card. Receipt of the PAN is a request to write a token to the MasterCard token vault. The token will thereafter be associated with the customer's PAN. In this way, the token is "metadata"—i.e., the data (token) about the data (PAN).

b. Claim 12 has "an authentication module, the authentication module authenticating the membership verification token, the authentication being performed in connection with a token database . . . ." (Ex. B, 16:11-14.) After Discover receives the McDonald's customer's PAN, Discover uses the authentication module to authenticate the PAN with the issuer of the card.

c. Claim 12 also has "a connection module, the connection module establishing a connection with the at least one communications console, wherein the communications console is a combination of a graphic user interface (GUI) and an Application Programmable Interface (API)

protocol wherein the API is related to a verified web service, the verified web service capable of facilitating a two way data exchange to complete a verification process . . . .” (Ex. B, 16:15-22.) After Discover has authenticated the McDonald’s customer’s PAN, Discover uses the connection module to establish a connection between the Discover payment processor and Discover’s token service provider. This API communication is possible because Discover has been issued and assigned a “Token Requestor ID” per the EMVCo Tokenization Specification.

d. In claim 12, there is “a request module, the request module requesting at least one electronic identification reference from the at least one communications console wherein the electronic identification reference comprises a verified web service account identifier of the first user . . . .” (Ex. B, 16:23-27) The Discover payment processor uses the API connection with the token servicer provider to request the token associated with the customer’s PAN.

e. Claim 12 includes “a second receipt module, the second receipt module receiving the at least one electronic identification reference from the at least one communications console . . . .” (Ex. B, 16:28-30.) The token is received by the payment processor from the token service provider.

f. Claim 12 has “a branding module, the branding module branding metadata of the encrypted digital media by writing the membership verification token and the electronic identification reference into the metadata.” (Ex. B, 16:31-34.) Discover writes the token to the token vault, associating the

token to the PAN for later cross-referencing upon subsequent hamburger purchases at this McDonald's.

Damages

21. McDonald's knows of the '860 patent and the '555 patent based on, among other things, correspondence between Mr. Grecia's counsel and McDonald's. Moreover, McDonald's knows how the '860 patent and '555 patent claims read on McDonald's use of the Visa, AMEX, MasterCard, and Discover tokenization systems, as Mr. Grecia's counsel provided a claim chart to McDonald's and discussed the claim chart with counsel to McDonald's. Notwithstanding this particular knowledge of how McDonald's use infringes the '860 patent and the '555 patent, McDonald's refuses to license the '860 patent and the '555 patent. In sum, McDonald's willfully infringes the '860 patent and the '555 patent.

22. Mr. Grecia has filed lawsuits against Visa, AMEX, and MasterCard based on those companies' infringements of U.S. Patent No. 8,887,308, the '860 patent, and the '555 patent (together, the "Portfolio"). In January 2015, Grecia disclosed the Portfolio to each of Visa, AMEX, and MasterCard, explaining why these companies infringed and offering a license. The royalty Grecia seeks from McDonald's is a percentage of the fees that McDonald's currently pays Visa, AMEX, MasterCard, and Discover for unauthorized use of Mr. Grecia's claimed systems.

WHEREFORE, Grecia respectfully requests that this Court enter judgment against McDonald's as follows:

A. Finding that McDonald's has infringed and is infringing one or more claims of the '860 patent and the '555 patent;

B. Finding that McDonald's' infringement has been willful;

C. Awarding a reasonable royalty, including pre-judgment and post-judgment interest;

D. Awarding treble damages;

E. Finding that this case is "exceptional" under 35 U.S.C. § 285 and awarding Grecia his expenses and attorneys' fees incurred in bringing and prosecuting this action; and,

F. Awarding such additional relief as the Court deems just and proper.

Jury Demand

Under Rule 38(b) of the Federal Rules of Civil Procedure, Mr. Grecia requests a trial by jury.

Date: February 24, 2016

Respectfully submitted,

/s/ Matthew M. Wawrzyn

Matthew M. Wawrzyn (#6276135)
mwawrzyn@siprut.com
Stephen C. Jarvis (#6309321)
sjarvis@siprut.com
Richard S. Wilson (#6321743)
rwilson@siprut.com
SIPRUT PC
17 North State Street, Suite 1600
Chicago, IL 60602
Telephone: 312.236.0000
Fax: 312.878.1342

Counsel for William Grecia