Court File No. CV-16-11290-00CL

ONTARIO
SUPERIOR COURT OF JUSTICE
COMMERCIAL LIST

IN THE MATTER OF MAPLE BANK GmbH

AND IN THE MATTER OF THE *WINDING-UP AND RESTRUCTURING ACT*,
R.S.C. 1985, C.W-11, AS AMENDED

AND IN THE MATTER OF THE *BANK ACT*, S.C. 1991, C.46, AS AMENDED

B E T W E E N:

THE ATTORNEY GENERAL OF CANADA

Applicant

and

MAPLE BANK GMBH

Respondent

AFFIDAVIT OF DR. CHARLOTTE SCHILDT
(Sworn December 7, 2017)

I, DR. CHARLOTTE SCHILDT, of the City of Frankfurt, Germany, MAKE OATH AND SAY:

1. I am a partner at CMS Hasche Sigle, counsel to Dr. Michael C. Frege, the German court-appointed insolvency administrator (the "**GIA**") of Maple Bank GmbH ("**Maple Bank**").

2. This affidavit is filed in connection with the motion by KPMG Inc., in its capacity as Liquidator (the "**Liquidator**") of the Canadian branch of Maple Bank (the "**Canadian Branch**"), for an order (the "**Production Order**") authorizing and directing the Liquidator to produce, transfer or release the Information (as defined below) to the GIA and granting other related relief.

Background on the Role and Duties of the GIA

3. The GIA was appointed as the insolvency administrator of Maple Bank pursuant to an order of the German Insolvency Court dated February 11, 2016. One of the core principles in German insolvency proceedings is the principle of universality. This means that the insolvent estate falling within the jurisdiction of the German insolvency regime consists of all assets of the debtor, wherever located. The Canadian Branch is part of Maple Bank and not a separate legal entity. Therefore, as a matter of German law, and notwithstanding the appointment of the Liquidator, the appointment of the GIA extends to the Canadian Branch.

4. German law specifically provides for the appointment, rights and duties of the GIA. The GIA is required by either statute or court decisions to, among other things:

(a) administer, dispose of and distribute the insolvency estate of the debtor, wherever those assets are located;

(b) treat all creditors equally;

(c) take protective actions to preserve the assets of the debtor wherever required;

(d) collect, safeguard and assess information of the debtor, its branches and subsidiaries, including their books and records whether in electronic or physical form;

(e) assess filed claims by creditors, including the tax authority, and assess potential liability, damage, clawback or repayment claims;

(f) work cooperatively with the German tax authorities and German prosecutors in accordance with German jurisprudence;

(g) make a proper and timely declaration of taxes for the debtor, disclose facts to the tax authority and prosecutors and assess whether tax returns submitted by the debtor in the past must be corrected as provided for by German law;

(h) prepare the annual returns for the debtor in a timely manner and provide data and information to the appointed auditors, including information regarding the debtor's branches and subsidiaries;

(i) protect the interests of each creditor, including the tax authority, in an equal manner; and

(j) be independent and neutral and act in the best interests of the creditors in their entirety in accordance with their respective rights.

The GIA is, by virtue of law and the order commencing the German Insolvency Proceeding, an organ of the administration of justice. I understand that this concept is similar to the Canadian concept of an "Officer of the Court". Under the principle of universality, its rights and duties as such under German law extend to the Canadian Branch.

5. The insolvency proceeding in Germany regarding Maple Bank was commenced following a moratorium imposed on Maple Bank by the German Federal Financial Supervisory Authority (the "**German Insolvency Proceeding**"). This moratorium was imposed following the commencement in Germany of a criminal and tax investigation in relation to former directors, supervisory board members, officers and former employees of Maple Bank involving allegations of serious tax evasion and money-laundering.

6. The German tax authority has filed substantial claims in the aggregate amount of more than EUR 500 million in the German Insolvency Proceeding for repayment of tax refunds and associated interest.

7. Some of the transactions being investigated or assessed may have involved the Canadian Branch and affiliates of Maple Bank (the "**Affiliated Companies**"). The investigations and assessments with respect to the various transactions and relationships are ongoing.

Information Request from the GIA

8. The GIA has become aware that the Liquidator has in its power, possession or control transaction records, documents, emails, other communications and other information or data (the "**Information**") relating to, *inter alia*, transactions entered into by Maple Bank, acting through its Canadian Branch, including transactions among the Canadian Branch and the Affiliated Companies (the "**Maple Bank Group**"). The GIA is seeking to obtain the Information in order to fulfill his duties as described above, in particular to fulfill his statutory and legal duties under German law with respect to the (a) collection, safeguarding and assessment of information of the insolvent parties, (b) satisfaction of tax filing, annual return filing and other compliance and disclosure or correction obligations of Maple Bank to tax authorities, banking authorities or German prosecutors, (c) investigation of potentially improper conduct within the Maple Bank Group with respect to liability, damage, clawback

and repayment claims and (d) obligation to cooperate with and respond to the investigation by tax authorities and German prosecutors with respect to their respective investigations and requirements. To this end, the GIA has requested that the Liquidator provide him with a complete copy of the Information (the "**Information Request**").

9. The GIA understands that much of the Information is in electronic form and is resident in a data processing services centre owned by Sungard Availability Services (Canada) Ltd. located at 2330 Argentia Road, Mississauga, Ontario (the "**Sungard Facility**"). There are also physical documents which are located at facilities owned by Record Xpress Inc., located at 124 Crockford Boulevard, Scarborough, Ontario, M1R 3C3 (the "**Record Xpress Facility**") and at facilities owned by Iron Mountain, located at 195 Summerlea Road, Brampton, Ontario L6T 4P6 (the "**Iron Mountain Facility**"). The SunGard, Record Xpress and Iron Mountain contracts were all entered into by Maple Securities Canada Limited ("**MSCL**"). In order to effectively access the data in electronic form, the GIA will also need access to software, services and technical; equipment owned or licensed by MSCL or other affiliates.

10. The GIA has discussed its obligation to obtain data, documents and information, including any software, services or technical equipment required to access such data, with the Liquidator, with Deloitte Restructuring Inc. ("**Deloitte**") in its capacity as trustee in bankruptcy (the "**Trustee**") of Maple Bank's indirect parent company, Maple Financial Group Inc. ("**MFGI**") and in its capacity as receiver (the "**Receiver**") of MFGI's direct subsidiary, Maple Futures Corp. ("**MFC**") and with MSCL, Maple Bank's direct subsidiary.

11. The GIA understands from such discussions that the Liquidator and the Trustee have obtained on tapes duplicate copies of the electronic Information stored at the Sungard Facility.

12. The GIA and Liquidator have worked collaboratively to arrive at a basis upon which the Information can be provided to the GIA that:

(a) allows the GIA to perform its duties and obligations under German law;

(b) respects the rights of the GIA;

(c) provides reasonable protection to any individual whose personal information may be included in the Information; and

(d) provides protection to the Liquidator.

Position of the GIA

13. The GIA takes the position that:

(a) granting the Production Order is consistent with the terms of the Winding-Up Order;

(b) the principles of comity favour the sharing of the Information with another court officer who requires the Information for the proper administration of the Maple Bank GmbH estate;

(c) any privacy concerns related to the production of the Information are adequately addressed through, among other things, German privacy law; and

(d) attempting to segregate the Information and allocate information to various legal entities within the Maple Bank Group serves no valid purpose and would not be practicable.

(a) The Winding-Up Order

14. Subparagraph 8(a) of the Winding-Up Order provides that the Liquidator shall provide the GIA "such information regarding the Business and Assets of Maple Bank as the [GIA] may reasonably require in order to fulfill his statutory obligations under German law."

15. Paragraph 9 of the Winding-Up Order further provides that "the Liquidator and the [GIA] shall consult and exchange information in respect of the Assets and Business of Maple Bank in Canada and such assets and business of Maple Bank as may be connected thereto, all as may be required for the effective and efficient administration of Maple Bank in Canada [the Canadian Branch] and Maple Bank."

(b) Comity

16. The GIA asks the court to consider principles of international comity in insolvency proceedings and recognize the rights and obligations of the GIA, as a foreign court-appointed officer, including the duty to collect, safeguard and assess information of the insolvent parties, including their books and records. The Canadian Court has, itself, invoked comity in the Winding-Up Order at paragraph 34, where it requests the aid and recognition of foreign courts, including the Amtsgericht Frankfurt am Main [Insolvency Court] in the Federal Republic of Germany, and at paragraph 35, where it requests the aid and assistance of the GIA.

(c) Any Privacy Concerns are adequately addressed

17. The circumstances with respect to the data are such that there would be a diminished expectation of privacy with respect to any employees in Canada of the Maple Bank Group. To the extent that any expectation of privacy exists in respect of such employees or other persons, it would be adequately protected by German privacy law and the non-public nature of the German Insolvency Proceeding

(i) Diminished expectations of privacy for employees

18. From his discussions with the Liquidator, the GIA understands that the Canadian Branch had a Computer Network and Internet Usage Policy (the "**Network and Internet Policy**") and an email policy (the "**Email Policy**"), copies of which are attached hereto as **Exhibits "A"** and **"B"**, respectively.

The Network and Internet Policy included the following statements:

(a) "...All such information, content and files are the property of the Company. You should have no expectation of privacy regarding them..." (see Privacy section); and

(b) "...The Company reserves the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the Network and the Internet as well as any and all materials, files, information, software, communications and other content transmitted, received or store in connection with this usage..." (see Privacy section).

The Email Policy includes the following statements:

(a) "Employees may use email to communicate with spouses, children, domestic partners and other family members" (see Authorized Personal Use of Email section);

(b) "Email messages created and transmitted on Company computers are the property of the Company..." (see Employees Have No Reasonable Expectation of Privacy section); and

(c) "...Employees have no reasonable expectation of privacy when it comes to business and personal use of the Company's email system." (See Employees Have No Reasonable Expectation of Privacy section).

The GIA understands that these policies were made available to all employees in Canada of the Maple Bank Group on the Maple Bank Group website. Accordingly, Canadian employees did not have a reasonable expectation of privacy (or, in the alternative, any reasonable expectation of privacy was significantly diminished). In

any event, I believe that the large majority of the Information would consist of work related emails and documents, and not personal information.

19. The Information may also contain customer information related to mortgage loans and immigrant investor loans made by the Canadian Branch to individuals. Information of this nature is not central to the GIA's request and if it can be efficiently excluded from the Production Order, and without delaying the production of the other information the GIA would not object to such exclusion.

20. For the reasons set out below, to the extent such information cannot be efficiently excluded, or such exclusion would delay the production, then the mortgage loan and immigration investor loan information should be included in the Production Order. Production of the Information should not be delayed. If the mortgage loan and immigration investor loan is so included, it would benefit from the privacy and confidentiality protections set out below.

(ii) German privacy law adequately addresses privacy concerns

21. The GIA is subject to significant privacy obligations under German Law. These obligations are at least as onerous as the privacy obligations that arise under Canadian law. Any personal information disclosed to the GIA will be subject to privacy protection under German law. German Data Protection Law is essentially regulated in the German Federal Data Protection Act (*Bundesdatenschutzgesetz* - "**BDSG**"); an unofficial translation of which, provided by the Bundesministerium der Justiz und fur Verbraucherschutz (the Federal Ministry of Justice and Consumer Protection), is available at https://www.gesetze-im-internet.de/englisch_bdsg/. Relevant provisions from the BDSG are attached hereto as **Exhibit "C".**

22. German Data Protection Law, in particular,

(a) covers the collection, processing and use of personal data, i.e., every form of handling personal data (section 1 (2), section 3 (1), (3) - (5) BDSG); (personal data is broadly defined as "any information concerning the personal or material circumstances of an identified or identifiable individual");

(b) applies to any collection, processing, use and transfer of personal data by legal entities ("data controllers") located in Germany – including, for the avoidance of doubt – any branch offices of such data controllers located in Germany, regardless of place of residence or nationality of employees or other natural persons whose personal data are collected, processed or used ("data subjects");

(c) generally prohibits the collection, processing use and transfer of personal data unless covered by a statutory authorization or a consent of the data subject (section 4 (1) BDSG);

(d) provides for statutory authorizations according to which the collection, processing and use of personal data is permitted to the extent necessary for compliance with legal obligations under applicable law (section 4 (1), (2) no. 1; section 28 (1) no. 2, (6) no. 3 BDSG);

(e) prohibits – on the basis of the general prohibition mentioned in section (c) above – also the transfer or disclosure of personal data to third parties without a statutory authorization or consent of the data subject; this also applies to the disclosure of personal data to local government authorities which may only be based on the strict mandatory requirements under applicable law (e.g. competences of criminal

prosecution authorities regularly requiring court orders for the seizure of documents/information);

(f) contains further obligations for every data controller (i.e. the legal entity collecting, processing or using personal data), including

(i) the information of data subjects on the collection, processing and use of their personal data (section 4 (3) BDSG),

(ii) the appointment of an independent data protection officer (section 4 f BDSG),

(iii) an explicit obligation of employees to confidentiality and data secrecy (section 5 BDSG),

(iv) the definition and application of appropriate technical and organisational measures to protect personal data against unauthorized access or processing and accidental loss (section 9 BDSG),

(v) an obligation to delete personal data if they are no longer necessary for the purpose for which it was collected; in case of mandatory retention requirements, the processing of personal data may be restricted before deletion (section 35 (2), (3) BDSG); and

(vi) as well as documentation and accountability requirements; and

(g) provides for control and enforcement of mandatory requirements by independent supervisory authorities (section 38 BDSG) and a sanctions regime (including administrative fines up to EUR 300,000 for a case of non-compliance, section 43 BDSG).

The European Commission has assessed the level of data protection in Canada prior to issuing its "adequacy decision" (http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002D0002&from=EN) confirming that the Canadian Personal Information Protection and Electronic Documents Act provides an adequate protection compared to the requirements on the EU Data Protection Directive (95/46/EC) on the basis of which national data protection laws in the EU member states (including the BDSG) were enacted.

(iii) Non-public nature of the German Insolvency Proceeding and laws on Banking Secrecy

23. The German Insolvency Proceeding is, by virtue of law, a non-public proceeding (an "in camera" proceeding). Moreover, German laws relating to banking secrecy as well as insolvency and tax secrecy apply to the German Insolvency Proceeding. The GIA owes reporting duties to the Insolvency Court supervising the GIA, the court-appointed creditors committee members (each of whom have signed express confidentiality declarations) as well as the German banking regulator according to the German Banking Act (Kreditwesengesetz – "**KWG**"). According to German statutory law, only creditors of Maple Bank have a right to access the files of the Insolvency Court. All regular reporting to creditors by the GIA is consistent with the applicable laws on secrecy and privacy.

(iv) Other standards under German law

24. Any access by German prosecutors to any data or documents retrieved from Canada would be pursuant to an order of the German court. Reporting or disclosure vis-à-vis German authorities, in particular, the tax authorities would be based on German law requirements or the obligations of Maple Bank as taxpayer.

(d) Segregation of Information is disproportionate in the circumstances

25. The GIA understands that the Information may include information relating to:

(a) MFGI;

(b) Maple Banks' direct subsidiary, MSCL, which is being wound up outside of any court proceeding under the corporate law dissolution provisions contained in the *Canada Business Corporations Act*; and

(c) the Affiliated Companies.

In some cases the Information may relate to the Canadian Branch alone. In other cases it may relate to the Canadian Branch and entities of the Maple Bank Group. In other cases it may relate to one or more other Maple Bank Group entities, and not the Canadian Branch. For instance, emails may be sent or received by shared employees and transactions may involve more than one entity in the Maple Bank structure. A case-by-case review and any segregation or allocation would be prohibitively expensive and time consuming, and likely impossible in practice. The GIA believes that there would be no way to make this determination except on a case by case, document by document basis, which would be exceptionally time-consuming and the cost of which would be disproportionate.

26. Maple Bank is the parent of each entity in the Maple Bank Group with the exception of MFGI and its direct parent company Maple Financial Europe SE ("**Maple SE**"). Although the GIA has been advised by MSCL that some of the information stored at the SunGard Facility, the Record Xpress Facility or the Iron Mountain Facility, respectively, may belong to MFGI or MSCL, it understands that the overwhelming majority may belong to the Canadian Branch.

27. Furthermore, the majority of personal information is likely related to individual mortgages, immigration loans to individuals and deposits – each a line of business operated exclusively in Canada by the Canadian Branch. Accordingly, any personal information likely belongs to the Canadian Branch.

28. The process of segregating personal information from the other Information, even if possible, would be extremely time consuming and expensive. The fees and expenses which would be associated with such a review of the documents are not proportionate to any privacy interests engaged in this matter.

29. Although the relief sought in the Production Order does not seek any production of Information from Deloitte, the Trustee or the Receiver (given that the Liquidator is in possession or control of all such Information), the GIA has discussed the Production Order with the Trustee and the Receiver since, as noted above, some of the Information that the Liquidator is required to produce under the Production Order could potentially include Information related or belonging to MFGI or MFC. The Trustee and the Receiver have requested that any persons who are likely to be affected by the Production Order, including MFGI shareholders, creditors, directors and employees, be served with the Liquidator's motion seeking the Production Order, so that such parties have an opportunity to object to the production of such Information. The Trustee and the Receiver have provided a list of such persons that they are aware of that may be affected by the Production Order and have advised that, on the basis of those persons being served with the motion, the Trustee and the Receiver do not object to the granting of the Production Order.

30. The GIA has discussed the Production Order with MSCL acting by its director. In connection with the ongoing wind-up of MSCL and its surrender of its membership in the Investment Industry Regulatory Organization of Canada ("**IIROC**"), MSCL provided an undertaking to IIROC dated August 10, 2016 (the "**IIROC Undertaking**") to provide IIROC with access to certain regulatory books

and records of MSCL, including certain information stored at the SunGard Facility, the Record Xpress Facility or the Iron Mountain Facility, for a period of seven years. In connection with the IIROC Undertaking, MSCL entered into a services agreement dated as of August 10, 2016 with EY pursuant to which EY agreed store certain electronic regulatory books and records of MSCL and to make such regulatory books and records available, upon request from IIROC. On the basis that (a) MSCL or the GIA will continue to store and make such regulatory books and records available upon request from IIROC and comply with the IIROC Undertaking, and (b) MSCL will continue to have access to the Data (i) in connection with the ongoing wind-up of MSCL for so long as MSCL remains in existence, or (ii) to the extent such access is required by applicable Canadian law, the GIA understands that MSCL consents to the Production Order in form and substance.

31. With respect to any information belonging to the Canadian Branch, the GIA believes that there is no "Disclosure" within the meaning of the word under PIPEDA because the Information remains within the same corporation - Maple Bank.

32. Accordingly, the GIA submits that it is appropriate that the Court grant the draft Production Order in the form attached as Schedule "B" to the Notice of Motion of the Liquidator dated December 6, 2017.

SWORN BEFORE ME at the City of Toronto, on December 7, 2017.

Commissioner for taking affidavits

Dr. Charlotte Schildt

This Affidavit was sworne before me by Dr. Charlotte Schildt, born on July 16, 1978 in Hamburg, German citizen, resident at CMS Hasche Sigle, Neue Mainzer Str. 2 - 4, 60311 Frankfurt am Main, Germany.

Dr. Frank Burmeister
Notary

DR. FRANK BURMEISTER NOTAR IN FRANKFURT AM MAIN

87626087v1

EXHIBIT "A"

This is **Exhibit "A"** to the

Affidavit of Dr. Charlotte Schildt

Sworn December 7, 2017

Commissioner for taking affidavits

Appendix A
October 30, 2017

Computer Network and Internet Usage Policy

The Company is pleased to offer access to the organization's computer Network and the Internet. This Policy applies to employees granted Network and Internet access by the Company. Upon acceptance of your account information and agreement to follow this Policy, you will be granted Network and Internet access. If you have any questions about the provisions of this Policy, you should contact your manager.

If you or anyone you allow to access your account (itself a violation of this Policy) violates this Policy, your access may be denied or withdrawn. In addition, you may be subject to disciplinary action, up to and including termination.

Personal Responsibility
By accepting your account password and related information, and accessing the Company's Network or Internet system, you agree to adhere to this Policy. You also agree to report any Network or Internet misuse to the Chief Information Officer. Misuse includes Policy violations that harm another person or another individual's property.

Term of Permitted Use
Network and Internet access extends throughout the term of your employment, provided you do not violate the organization's Computer Network and Internet Usage Policy. Note: The Company may suspend access at any time for technical reasons, Policy violations, or other concerns.

Purpose and Use
The Company offers access to its Network and Internet system for primarily business purposes. If you are unsure whether an activity constitutes appropriate business use, consult your manager.

Netiquette Rules
Employees must adhere to the rules of Network etiquette, or Netiquette. In other words, you must be polite, and use the Network and Internet appropriately and legally. The Company will determine what materials, files, information, software, communications, and other content and activity are permitted or prohibited, as outlined below.

Banned Activity
The following activities violate the Company's Computer Network and Internet usage Policy:

- Using, transmitting, receiving, or seeking inappropriate, offensive, vulgar, suggestive, obscene, abusive, harassing, belligerent, threatening, defamatory (harming another person's reputation by lies), or misleading language or materials.
- Engaging in illegal or inappropriate activities, violating the Employee Handbook, or encouraging others to do so. Examples:
  - Accessing others' folders, files, work, networks, or computers. Intercepting communications intended for others.
  - Downloading or transmitting the organization's confidential information or trade secrets.
- Causing harm or damaging others' property including downloading or transmitting copyrighted materials without permission from the copyright holder. Even when materials on the Network or the Internet are not marked with the copyright symbol, employees should assume all materials are protected under copyright laws – unless explicit permission to use the materials is granted.
- Jeopardizing the security of access, the Network, or other Internet Networks by disclosing or sharing passwords and/or impersonating others.
- Wasting the Company's computer resources. Do not send electronic chain letters. Do not send email copies to nonessential readers. Do not send email to group lists unless it is appropriate for everyone on a list to receive the email. Do not send organization-wide emails without your supervisor's permission.
- Connecting hardware to any computer or the Company's Network, or installing or upgrading software without the explicit permission of the IT department.

Confidential Information
Employees may have access to confidential information about the Company, our employees, and clients. With the approval of management, employees may use email to communicate confidential information internally to those with a need to know. When in doubt, do not use email to communicate confidential material. When a matter is personal, it may be more appropriate to send a hard copy, place a phone call, or meet in person.

Privacy
Network and Internet access is provided as a tool for our organization's business. The Company reserves the right to monitor, inspect, copy, review, and store at any time and without prior notice any and all usage of the Network and the Internet, as well as any and all materials, files, information, software, communications, and other content transmitted, received, or stored in connection with this usage. All such information, content, and files are the property of the Company. You should have no expectation of privacy regarding them. Network administrators may review files and intercept communications for any reason, including but not limited to maintaining system integrity and ensuring employees are using the system consistently with this Policy.

Noncompliance
Your use of the Network and the Internet is a privilege, not a right. Violate this policy and your access to the Network and the Internet may be terminated, perhaps for the duration of your tenure with the Company. Permitting another person to use your account or password to access the Network or the Internet – including but not limited to someone whose access has been denied or terminated – is a violation of Policy. Should another user violate this Policy while using your account, you will be held responsible, and both of you will be subject to disciplinary action. Criminal violations may lead to criminal or civil prosecution.

Employee Acknowledgment
Note: If you have questions or concerns about this Policy, contact your manager before signing this agreement.

I have read the Company's Computer Network and Internet Usage Policy and agree to abide by it. I understand violation of any of the above terms may result in discipline, up to and including my termination.

_____
User Name

_____
User Signature

_____
Date

EXHIBIT "B"

This is **Exhibit "B"** to the

Affidavit of Dr. Charlotte Schildt

Sworn December 7, 2017

Commissioner for taking affidavits

Appendix B
October 30, 2017

Email Policy

The Company provides employees with electronic communications tools, including an Email System. This written Email Policy, which governs employees' use of the Company's email system, applies to email use at the Company's headquarters and district offices, as well as at remote locations, including but not limited to employees' homes, airports, hotels, client and supplier offices. The Company's email rules and policies apply to full-time employees, part-time employees, independent contractors, interns, consultants, suppliers, clients, and other third parties. Any employee who violates the Company's email rules and policies may be subject to disciplinary action, up to and including termination.

Email Exists for Business Purposes
The Company allows email access primarily for business purposes. Employees may use the Company's email system for personal use only in accordance with this policy.

Authorized Personal Use of Email
Employees may use email to communicate with spouses, children, domestic partners, and other family members. Employees' personal use of email should be limited and reasonable. Employees are prohibited from using email to operate a business, conduct an external job search, solicit money for personal gain, campaign for political causes or candidates, or promote or solicit funds for a religious or other personal cause unless explicitly authorized by their manager.

Employees Have No Reasonable Expectation of Privacy
Email messages created and transmitted on Company computers are the property of the Company. The Company reserves the right to monitor all email transmitted via the Company's computer system. Employees have no reasonable expectation of privacy when it comes to business and personal use of the Company's email system.

The Company reserves the right to Monitor, Inspect, Copy, Review, and Store
at any time and without notice any and all usage of email, and any and all files, information, software, and other content created, sent, received, downloaded, uploaded, accessed, or stored in connection with employee usage. The Company reserves the right to disclose email text and images to regulators, the courts, law enforcement, and other third parties without the employee's consent.

Offensive Content and Harassing or Discriminatory Activities Are Banned
Employees are prohibited from using email to engage in activities or transmit content that is harassing, discriminatory, menacing, threatening, obscene, defamatory, or in any way objectionable or offensive.

Confidential, Proprietary, and Personal Information Must Be Protected
Unless authorized to do so, employees are prohibited from using email to transmit confidential information to outside parties. Employees may not access, send, receive, solicit, print, copy, or reply to confidential or proprietary information about the Company, employees, clients, suppliers, and other business associates. Confidential information includes but is not limited to client lists, credit card numbers, Social Insurance Numbers, employee performance reviews, salary details, trade secrets, passwords, and information that could embarrass the Company and employees were it to be made public.

Do Not Use Email to Communicate with Lawyers
In order to preserve the attorney-client privilege for communications between lawyers and clients, never use email to seek legal advice or pose a legal question.

Violations
These guidelines are intended to provide Company employees with general examples of acceptable and unacceptable use of the Company's email system. A violation of this policy may result in disciplinary action up to and including termination.

Acknowledgement
If you have questions about the above policies and procedures, address them to your manager before signing the following agreement.

I have read the Company's Email Policy and agree to abide by it. I understand that a violation of any of the above policies and procedures may result in disciplinary action, up to and including my termination.

_____
User Name

_____
User Signature

_____
Date

EXHIBIT "C"

This is **Exhibit "C"** to the

Affidavit of Dr. Charlotte Schildt

Sworn December 7, 2017

Commissioner for taking affidavits

EXHIBIT "C"
BDSG PROVISIONS

Federal Data Protection Act in the version promulgated on 14 January 2003 (Federal Law Gazette I p. 66), as most recently amended by Article 1 of the Act of 14 August 2009 (Federal Law Gazette I p. 2814)

Section 1
Purpose and scope

...

(2) This Act shall apply to the collection, processing and use of personal data by

1. public bodies of the Federation,

2. public bodies of the Länder in so far as data protection is not governed by Land legislation and in so far as they

   a) execute federal law or,

   b) act as bodies of the judicature and are not dealing with administrative matters,

3. private bodies in so far as they process or use data by means of data processing systems or collect data for such systems, process or use data in or from non-automated filing systems or collect data for such systems, except where the collection, processing or use of such data is effected solely for personal or family activities.

...

Section 3
Further definitions

(1) "Personal data" means any information concerning the personal or material circumstances of an identified or identifiable individual (the data subject).

...

(3) "Collection" means the acquisition of data on the data subject.

(4) "Processing" means the storage, modification, transfer, blocking and erasure of personal data. In particular cases, irrespective of the procedures applied:

1. "storage" means the entry, recording or preservation of personal data on a storage medium so that they can be processed or used again,

2. "modification" means the alteration of the substance of stored personal data,

3. **"transfer"** means the disclosure to a third party of personal data stored or obtained by means of data processing either

   a) through transmission of the data to the third party or

   b) through the third party inspecting or retrieving data held ready for inspection or retrieval,

4. "blocking" means labelling stored personal data so as to restrict their further processing or use,

5. "erasure" means the deletion of stored personal data.

(5) "Use" means any utilization of personal data other than processing.

...

Section 4
Admissibility of data collection, processing and use

(1) The collection, processing and use of personal data shall be admissible only if permitted or prescribed by this Act or any other legal provision or if the data subject has consented.

(2) Personal data shall be collected from the data subject. They may be collected without his/her participation only if

1. a legal provision prescribes or peremptorily presupposes such collection or

...

and there are no indications that overriding legitimate interests of the data subject are impaired.

(3) If personal data are collected from the data subject, the controller is to inform him/her as to

1. the identity of the controller,

2. the purposes of collection, processing or use and

3. the categories of recipients only in so far as the circumstances of the individual case provide no grounds for the data subject to assume that data will be transferred to such recipients,

unless the data subject has already acquired such knowledge by other means. If personal data are collected from the data subject pursuant to a legal provision which makes the supply of particulars obligatory or if such supply is the prerequisite for the granting of legal benefits, the data subject shall be informed that such supply is obligatory or voluntary, as the case may be. In

so far as the circumstances of the individual case dictate or at the data subject's request, he/she shall be informed of the legal provision and of the consequences of withholding particulars.

Section 4f
Data protection official

(1) Public and private bodies which process personal data automatically shall appoint in writing a data protection official. Private bodies are obliged to appoint such an officer within one month of commencing their activities. The same shall apply where personal data are processed by other means and at least 20 persons are permanently employed for this purpose. The first and second sentences above shall not apply to private bodies which generally deploy a maximum of nine employees to carry out the automatic processing of personal data on an ongoing basis. In so far as the structure of a public body requires, the appointment of one data protection official for several areas shall be sufficient. In so far as private bodies carry out automated processing operations which are subject to prior checking or process personal data in the course of business for the purposes of transfer, anonymized transfer, or market or opinion research, they are to appoint a data protection official irrespective of the number of persons deployed to carry out automatic processing.

(2) Only persons who possess the specialized knowledge and demonstrate the reliability necessary for the performance of the duties concerned may be appointed data protection official. The required level of specialized knowledge is determined in particular according to the scope of data processing carried out by the controller concerned and the protection requirements of the personal data collected or used by the controller concerned. A person from outside the body concerned may also be appointed data protection official; monitoring shall also extend to personal data which are subject to professional or official secrecy, in particular tax secrecy pursuant to Section 30 of the Fiscal Code.

(3) The data protection official shall be directly subordinate to the head of the public or private body. He or she shall be free to use his/her specialized knowledge in the area of data protection. He/she shall suffer no disadvantage through the performance of his/her duties. The appointment of a data protection official may be revoked by applying Section 626 of the Civil Code mutatis mutandis or, in the case of private bodies, at the request of the supervisory authority. If a data protection official is to be appointed under sub-Section 1, then this appointment shall not be subject to termination, unless there is reason for the controller to terminate the appointment for just cause without complying with a notice period. After the data protection official has been removed from office, he or she cannot be terminated for a year following the end of the appointment unless the responsible body has just cause for termination without complying with a notice period. The controller shall enable the data protection official to take part in advanced training measures and shall assume the expense of such measures, in order for the data protection official to maintain the expertise needed to perform his/her tasks.

(4) The data protection official shall be bound to maintain secrecy on the identity of the data subject and on circumstances permitting conclusions to be drawn about the data subject, unless he/she is released from this obligation by the data subject.

(4a) In so far as the data protection official obtains knowledge of data in the course of his or her activities in connection with which a right of refusal to give evidence applies on professional grounds to the head of the public or private body or a person employed at such a body, this right shall also apply to the data protection official and his/her assistants. The person to whom the right of refusal to give evidence applies on professional grounds shall decide whether to exercise this right, except where it will not be possible to effect such a decision in the foreseeable future. To the extent to which the data protection official's right of refusal to give evidence applies, the data protection official's files and other documentation shall be subject to a prohibition of seizure.

(5) The public and private bodies shall support the data protection official in the performance of his/her duties and in particular, to the extent needed for such performance, make available assistants as well as premises, furnishings, equipment and other resources. Data subjects may approach the data protection official at any time.

Section 5
Confidentiality

Persons employed in data processing shall not collect, process or use personal data without authorization (confidentiality). On taking up their duties such persons, in so far as they work for private bodies, shall be required to give an undertaking to maintain such confidentiality. This undertaking shall continue to be valid after termination of their activity.

Section 9
Technical and organizational measures

Public and private bodies processing personal data either on their own behalf or on behalf of others shall take the technical and organizational measures necessary to ensure the implementation of the provisions of this Act, in particular the requirements set out in the annex to this Act. Measures shall be required only if the effort involved is reasonable in relation to the desired level of protection.

Section 28
Collection and storage of data for own commercial purposes

(1) The collection, storage, modification or transfer of personal data or their use as a means of fulfilling one's own business purposes shall be admissible

...

2. in so far as this is necessary to safeguard justified interests of the controller of the filing system and there is no reason to assume that the data subject has an overriding legitimate interest in his data being excluded from processing or use,

...

In connection with the collection of personal data, the purposes for which the data are to be processed or used are to be stipulated in concrete terms.

...

(6) The collection, processing and use of special types of personal data (Section 3 (9)) for own commercial purposes shall be admissible when the data subject has not consented in accordance with Section 4a (3) if

...

3. this is necessary in order to assert, exercise or defend legal claims and there is no reason to assume that the data subject has an overriding legitimate interest in excluding such collection, processing or use, or

...

Section 35
Correction, erasure and blocking of data

...

(2) Personal data may be erased at any time, except in the cases specified in sub-Section 3, Nos. 1 and 2. Personal data in filing systems shall be erased if

1. their storage is inadmissible,

2. they concern information on racial or ethnic origin, political opinions, religious or philosophical convictions, union membership, health, sex life, criminal offences or administrative offences and the controller is unable to prove their accuracy,

3. they are processed for one's own purposes, as soon as knowledge of them is no longer needed for fulfilling the purpose for which they are stored, or

4. they are processed commercially for the purpose of transfer and an examination at the end of the fourth calendar year, for data concerning matters that have been concluded and the data subject does not object at the end of the third calendar year after the data were first stored, if an examination shows that further storage is unnecessary.

Personal data stored on the basis of Section 28a (2) first sentence or Section 29 (1) first sentence No. 3 shall be erased at the data subject's request.

(3) Instead of erasure, personal data shall be blocked where

1. in the case of sub-Section 2 second sentence No. 3 above, retention periods prescribed by law, statutes or contracts rule out any erasure,

2. there is reason to assume that erasure would impair legitimate interests of the data subject or

3. erasure is not possible or is only possible with disproportionate effort due to the specific type of storage.

...

Section 38
Supervisory authority

(1) The supervisory authority shall monitor implementation of this Act and other data protection provisions governing the automated processing of personal data or the processing or use of personal data in or from non-automated filing systems, including the rights of the member states in the cases under Section 1 (5) of this Act. It shall advise and support the data protection officials and the controllers with due regard to their typical requirements. The supervisory authority may process and use the data which it stores for supervisory purposes only; Section 14 (2), Nos. 1 to 3, 6 and 7 shall apply mutatis mutandis. The supervisory authority may, in particular, transfer data to other supervisory authorities for supervisory purposes. On request, it shall provide supplementary assistance to other Member States of the European Union (administrative assistance). If the supervisory authority establishes a breach of this Act or other data protection provisions, it shall be authorized to notify the data subjects accordingly, to report the breach to the bodies responsible for prosecution or punishment and, in cases of serious breaches, to notify the trade supervisory authority in order to initiate measures under industrial law. It shall publish an activity report on a regular basis, but at least every two years. Section 21 first sentence and Section 23 (5) sentences 4 to 7 shall apply mutatis mutandis.

(2) The supervisory authority shall keep a register of the automated processing operations which are subject to obligatory registration in accordance with Section 4d, stating the information specified in Section 4e first sentence. The register shall be open to inspection by any person. The right to inspection shall not extend to the information in accordance with Section 4e, sentence 1, No. 9 or stipulation of the persons entitled to access.

(3) The bodies subject to monitoring and the persons responsible for their management shall provide the supervisory authority on request and without delay with the information necessary for the performance of its duties. A person obliged to provide information may refuse to do so where he/she would expose himself or one of the persons designated in Section 383 (1), Nos. 1 to 3, of the Code of Civil Procedure to the danger of criminal prosecution or of proceedings under the Administrative Offences Act. This shall be pointed out to the person obliged to provide information.

(4) The persons appointed by the supervisory authority to exercise monitoring shall be authorized, where necessary for the performance of the duties of the supervisory authority, to enter the property and premises of the body during business hours and to carry out checks and inspections there. They may inspect business documents, especially the list stipulated in Section 4g (2) first sentence of this Act as well as the stored personal data and the data processing programs. Section 24 (6) of this Act shall apply mutatis mutandis. The person obliged to provide information shall permit such measures.

(5) To guarantee compliance with this Act and other data protection provisions, the supervisory authority may order measures to rectify violations during the collection, processing or use of personal data or technical or organizational irregularities detected. In the event of serious violations or irregularities, especially those connected with a special threat to privacy, the supervisory authority may prohibit collection, processing or use, or the use of particular procedures if the violations or irregularities are not rectified within a reasonable period contrary to the order pursuant to the first sentence above and despite the imposition of a fine. The supervisory authority may demand the dismissal of the data protection official if he/she does not possess the specialized knowledge and demonstrate the reliability necessary for the performance of his/her duties.

(6) The Land governments or the bodies authorized by them shall designate the supervisory authorities responsible for monitoring the implementation of data protection within the area of application of this Part.

(7) The Industrial Code shall continue to apply to commercial firms subject to the provisions of this Part.

Section 43
Administrative offences

(1) An administrative offence shall be deemed to have been committed by anyone who, whether intentionally or through negligence,

1. contrary to Section 4d (1), also in conjunction with Section 4e second sentence of this Act, fails to submit a notification, fails to do so within the prescribed time limit or fails to provide complete particulars,

2. contrary to Section 4f (1) first or second sentence of this Act, fails to appoint a data protection official or fails to do so within the prescribed time limit or in the prescribed manner,

2a. contrary to Section 10 (4) third sentence fails to ensure that data transfer can be ascertained and checked,

2b. contrary to Section 11 (2) second sentence fails to give the commission correctly, completely or in accordance with the rules, or contrary to Section 11 (2) fourth sentence fails to ensure prior to the processing of the data that technical and organizational measures taken by the agent are being complied with,

3. contrary to Section 28 (4) second sentence of this Act, fails to notify the data subject, or fails to do so within the prescribed time limit or in the prescribed manner, or fails to ensure that the data subject is able to obtain due knowledge,

3a. contrary to Section 28 (4) fourth sentence requires a stricter form,

4. transfers or uses personal data contrary to Section 28 (5) second sentence of this Act,

4a. contrary to Section 28a (3) first sentence fails to inform or fails to do so correctly, completely or within the prescribed time limits,

5. contrary to Section 29 (2) third or fourth sentence of this Act, fails to record the reasons described there or the means of credibly presenting them,

6. incorporates personal data into electronic or printed address, telephone, classified or similar directories contrary to Section 29 (3) first sentence of this Act,

7. contrary to Section 29 (3) second sentence of this Act, fails to ensure the adoption of labels,

7a. contrary to Section 29 (6) fails to handle an information request properly,

7b. contrary to Section 29 (7) first sentence fails to inform a consumer or fails to do so correctly, completely or within the prescribed time limits,

8. contrary to Section 33 (1) of this Act, fails to notify the data subject or fails to do so correctly or completely,

8a. contrary to Section 34 (1) first sentence, also in conjunction with sentence 3, contrary to Section 34 (1a), contrary to Section 34 (2) first sentence, also in conjunction with sentence 2, or contrary to Section 34 (2) fifth sentence, (3) first or second sentence, or (4) first sentence, also in conjunction with sentence 2 fails to provide information or fails to do so correctly, completely or within the prescribed time limits, or contrary to Section 34 (1a) fails to store data,

8b. contrary to Section 34 (2) third sentence fails to transmit information or fails to do so correctly, completely or within the prescribed time limits,

8c. contrary to Section 34 (2) fourth sentence fails to refer the data subject to the other body, or fails to do so within the prescribed time limits,

9. contrary to Section 35 (6) third sentence of this Act, transfers data without a counter-statement,

10. contrary to Section 38 (3) first sentence of this Act, fails to provide information or fails to do so correctly, completely or within the prescribed time limit or fails to permit a measure

11. fails to comply with an executable instruction under Section 38 (5) first sentence of this Act.

(2) An administrative offence shall be deemed to have been committed by anyone who, whether intentionally or through negligence,

1. collects or processes personal data which are not generally accessible without authorization,

2. holds personal data which are not generally accessible ready for retrieval by means of an automated procedure without authorization,

3. retrieves personal data which are not generally accessible or obtains such data for themselves or another from automated processing operations without authorization,

4. obtains by means of incorrect information the transfer of personal data which are not generally accessible,

5. contrary to Section 16 (4) first sentence, Section 28 (5) first sentence of this Act, also in conjunction with Section 29 (4), Section 39 (1) first sentence or Section 40 (1) of this Act, uses data for other purposes by transmitted them to third parties, or

5a. contrary to Section 28 (3b) makes concluding a contract dependent on the consent of the data subject,

5b. contrary to Section 28 (4) first sentence processes or uses data for purposes of advertising or market or opinion research,

6. contrary to Section 30 (1) second sentence, Section 30a (3) third sentence, Section 40 (2) third sentence of this Act, combines a characteristic mentioned there with specific information, or

7a. contrary to Section 42a first sentence fails to notify or fails to do so correctly, completely or within the prescribed time limit.

(3) Administrative offences shall be punishable by a fine of up to € 50,000 in case of sub-Section 1 above, and by a fine of up to € 300,000 in the cases under sub-Section 2 above. The fine shall exceed the financial benefit to the perpetrator derived from the administrative offence. If the amounts mentioned in the first sentence are not sufficient to do so, they may be increased.

IN THE MATTER OF THE MAPLE BANK GMBH

AND IN THE MATTER OF THE *WINDING-UP AND RESTRUCTURING ACT*,R.S.C. 1985, C.W-11, AS AMENDED

AND IN THE MATTER OF THE *BANK ACT*, S.C. 1991, C.46, AS AMENDED

Court File No: CV-16-11290-00CL

ONTARIO
SUPERIOR COURT OF JUSTICE
COMMERCIAL LIST

Proceeding commenced at Toronto

AFFIDAVIT OF DR. CHARLOTTE SCHILDT
(SWORN DECEMBER 7, 2017)

STIKEMAN ELLIOTT LLP
Barristers & Solicitors
5300 Commerce Court West
199 Bay Street
Toronto, Canada M5L 1B9

David Byers LSUC#: 22992W
Tel: (416) 869-
Fax: (416) 947-0866

C. Haddon Murray LSUC#: 61640P
Tel: (416) 869-5239
Fax: (416) 947-0866

Lawyers for the
German Insolvency Administrator