HFWC Privacy Policy

Published Privacy Policy

1.1.1 HFWC's Privacy Policy is attached as APPENDIX E as is published and distributed to clients and employees/agents of the firm. The Privacy Policy is available on HFWC's website.

1.2 Privacy Breach Policy and Procedures

1.2.1 HFWC has instituted best practices regarding privacy breach reporting. We are subject to the *Personal Information and Electronic Documents Act* ("PIPEDA") only in those provinces which do not have substantially similar legislation (including both BC and Alberta, where the *Personal Information Protection Act* ("PIPA") applies).

1.2.2 These best practices include that we must:

- **Report** to the Privacy Commissioner of Canada breaches of security safeguards involving personal information that pose a real risk of significant harm to individuals
- Volunteer cyber incident reporting to regulatory bodies
- **notify** affected individuals about those breaches, and
- keep **records** of all breaches.
- Conduct cyber security training (*the course is required to be completed by all HFWC registered and non-registered personne*l).

1.2.3 A breach of security safeguards is defined in PIPEDA as: the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards, or from a failure to establish those safeguards.

1.2.4 A breach involving personal information under HFWC control is required to be reported to the OPC if it is reasonable, under the circumstances, to believe that the breach creates a real risk of significant harm ("RROSH") to an individual. If it is HFWC's assessment that it creates a real risk of significant harm to an individual, whether the breach may impact one individual or hundreds, we must report it.

1.2.5 RROSH assessment includes factors such as the sensitivity of the

personal information involved in the breach and the probability the personal information has been/is/will be misused. “Significant harm” includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business, or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property. For HFWC personal client information, the most likely risk of harm will be identity theft or financial loss (i.e. unscrupulous parties using client information for identity theft purposes or to impersonate a client to attempt to withdraw/transfer out/endanger client funds). See the OPC website for specific guidance in Part 6 – Assessing real risk of significant harm (link at the end of this section).

1.2.6 Reporting to the Office of the Privacy Commissioner of Canada (“OPC”) is done by way of PIPEDA breach report form, with the CCO responsible for filing same, available at:

Go to "www.priv.gc.ca" and "report a concern" to find the link to Report a Breach

1.2.7 HFWC is obliged to notify individuals if we believe that the breach creates a real risk of significant harm to that individual. This notification assessment will be performed by the CCO and documented as part of our records, and if the CCO determines to provide individual notification, then documenting the method of direct or indirect notification made, which will form part of our records. Notifications to individuals must include the following information:

- a description of the circumstances of the breach;
- the day on which, or period during which, the breach occurred or, if neither is known, the approximate period;
- a description of the personal information that is the subject of the breach to the extent that the information is known;
- a description of the steps that the organization has taken to reduce the risk of harm that could result from the breach;
- a description of the steps that affected individuals could take to reduce the risk of harm that could result from the breach or to mitigate that harm; and
- contact information that the affected individual can use to obtain further information about the breach.

1.2.8 HFWC is required to keep records of all breaches, for a minimumtwo-yearr period. These records should include details about **all** breaches, whether they were determined as reportable or not. Records should at a

minimum contain the estimated or actual date of the breach; general description of the circumstances of the breach; the nature of information involved in the breach; whether or not the breach was reported to the OPC; and whether or not individuals were notified. The CCO is responsible for maintaining these records.

1.2.9 If we have notified individual(s) because of a real risk of significant harm, we should similarly report to certain organizations if we believe they can reduce or mitigate the risk of harm that can come from the breach. Examples for HFWC could include:

- Notifying law enforcement if there is an attack on our computer system where bad actors have accessed customers' information, if we believe law enforcement may be able to reduce the risk of harm that could result from the breach or mitigate the harm.

- Notifying our custodian(s), if we believe the organization may be able to reduce the risk of harm that could result from the breach or mitigate the harm.

1.2.10 Significant further guidance is available on the OPC website, under Home/Privacy Topics/Privacy Breaches/Respond to a privacy breach at your business