ivari is continuously monitoring our systems and security to safeguard our customer information. Our security teams receive alerts from a variety of cyber security intelligence sources including, but not limited to, the Canadian Centre for Cyber Security (CCCS), Computer Emergency Response Team (CERT), and the Financial Services – Information Sharing and Analysis Centre (FS-ISAC).

Earlier in December, a zero-day vulnerability was reported in a software component called Apache Log4j 2.x ("Vulnerability"). This software is widely used by many organizations around the world and this Vulnerability can allow attackers to gain unauthorized access to computer systems.

Upon becoming aware of this Vulnerability, ivari undertook the following actions:

1) Conducted a review of ivari's software code libraries and IT infrastructure to identify any vulnerable instances of Log4J and, where identified, ivari took actions to mitigate the Vulnerability;

2) Initiated contact with key third party software, hardware, and service partners to determine if their services and/or products were impacted by this Vulnerability and the status of their remediation effort; and

3) Worked with our Managed Security Services Provider (MSSP) to ensure all known indicators of compromise had been entered into the continuous monitoring and alerting systems. Both our MSSP and internal Security Teams remain on alert for suspicious activity.

Any known workarounds and patches for the Log4J Vulnerability have been implemented. In concert with ivari's software, hardware, and service partners, we are continuing to closely monitor the situation for new developments to ensure our systems and customer information remain secure. Contact PrivacyOffice@ivari.ca with any inquires.