Dear <<Name 1>>:

The Borough of Haledon Police Department ("Haledon") is writing to notify you of a recent event that may involve some of your information. Although at this time there is no indication that your information has been fraudulently misused in relation to this incident, we are providing you with information about the incident, our response to it, and additional measures you can take to protect your information, should you feel it appropriate to do so.

**What Happened?** On July 10, 2020, Haledon became aware of suspicious activity relating to its systems and immediately launched an investigation to determine the nature and scope of the activity. Haledon determined that an unknown actor gained access to certain Haledon systems on or about June 2, 2020. The unknown actor claimed to have removed certain databases from our network.

Although the investigation was unable to confirm which specific files, if any, were impacted, we could not rule out the possibility that some of your information may have been impacted. Therefore, in an abundance of caution because of the uncertainty of this event, Haledon undertook a comprehensive and time-intensive review of all files that could have been impacted. This review was recently completed and determined that your information was present in potentially impacted databases.

**What Information Was Involved?** Our investigation determined that at the time of the incident, your name and <<Breeched Elements>> were stored within potentially impacted databases. To date, Haledon has not received any reports of fraudulent misuse of any information potentially impacted by this event.

**What We Are Doing.** The confidentiality, privacy, and security of your information are among our highest priorities, and we have security measures in place to protect information in our systems. Upon learning of the activity, we immediately took steps to secure our systems and investigate the event. Haledon’s vendors deployed advanced endpoint monitoring tools to the network and secured access credentials in response to the event. We notified the Federal Bureau of Investigation of the event and assisted in its investigation. We are also notifying certain state regulators, as necessary.

While we are unaware of any fraudulent misuse of your information as a result of this incident, as an additional precaution, Haledon is offering you access to twelve (12) months of complimentary credit monitoring services through TransUnion. Details of this offer and instructions on how to activate these services are enclosed with this letter.

**What You Can Do.** We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Please also review the enclosed document, "Steps You Can Take to Help Protect Your Information," which contains information on what you can do to safeguard against possible misuse of your information. You can also enroll in the credit monitoring services that Haledon is offering to you.