Business email compromise incidents: Takeaways from IPC PHIPA Decision 205

July 10, 2023

In this article, we review a recent decision of the Information and Privacy Commissioner of Ontario (IPC) regarding the duty of an Ontario health information custodians to notify individuals affected by a business email compromise when there is no proof that personal health information was browsed or downloaded by a threat actor.

Background

Business email compromise incidents (BECs) are common in all sectors, including the Ontario health sector. They involve unauthorized access to one or more email accounts that may hold personal health information. The best practice in responding to a BEC is to retain a qualified third-party to conduct a forensic investigation with a view to determining whether the entire account was likely stolen or whether specific records in the account were likely browsed or downloaded.

"Likely" is a significant legal term that relates to the "balance of probabilities" standard of proof: proving something on a balance of probabilities means that it is more likely than not to have happened. Absent a presumption arising under statute or a rule of evidence, the balance of probabilities normally governs what is or is not "fact" in a legal proceeding.

Sometimes, a BEC forensic investigation will find evidence of browsing or downloading that meets the standard of proof. In such cases, PHIPA requires health information custodians to notify all individuals whose personal health information was browsed or downloaded (and report to the IPC), regardless of actual risk.

However, oftentimes a BEC forensic investigation will find no such proof. This could be due to an absence of evidence, or the evidence may be inconclusive in that it does not establish that browsing or downloading was "likely." There may also be evidence that weighs against a browsing or downloading conclusion – *e.g.*, evidence that suggests the threat actor's motive was to use the account as a phishing tool or to gather evidence to perpetrate a wire fraud rather than use the information in the account for financial or other gain. Browsing or downloading cannot be ruled out and is possible in this scenario but there may be indicators that weigh against the likelihood that personal health information was browsed or downloaded. In such cases, it is speculative whether

personal health information was actually browsed or downloaded and the most a custodian can rightly do is notify individuals that their personal health information "may have been browsed or downloaded without authorization."

Duty to notify and report

Under subsection 12 of *Personal Health Information Protection Act* (PHIPA), a health information custodian must notify individuals of privacy breaches at the first reasonable opportunity. A health information custodian must also report seven categories of breaches to the IPC, including breaches in which personal health information is stolen or if it is used or disclosed without lawful authority. If a BEC results in a privacy breach, it will always also require reporting to the IPC.

Decision 205

In Decision 205, an agent of a health information custodian suffered a BEC. The threat actor(s) accessed a single account without authorization and used it to send 2,000 phishing emails before the agent identified the problem and re-secured the account. The agent then hired a third-party to conduct a forensic investigation, which established that the threat actor accessed the account on four separate days. It does not appear that the investigator found any direct evidence of browsing or downloading, and it gave an affirmative (expert) opinion to the agent that the threat actor likely accessed the account to conduct a phishing campaign.

Nonetheless, the agent notified the custodian and reported the incident to the IPC, who directed the agent to notify. The IPC explains:

> [30] With respect to notification, the Agent advised that, on October 8, 2020, after the completion of the cybersecurity's investigation and despite having no reason to believe that PHI was accessed, copied or exfiltrated in the course of the phishing attack, it notified the Custodian of the outcome of the investigation and the steps that it took to contain and remediate the breach. The Agent also explained that it did not notify any affected individuals of the breach at the time because of this belief.
>
> [31] However, in light of the direction that it received from this office during the Intake Stage of the IPC's PHIPA complaint process regarding notification, the Agent advised that, in January and November 2022, it sent notification letters to 262 patients of the Custodian who were affected by the breach and one of these letters to its affected patient.

Later in Decision 205, the IPC accepted that the agent was "mistaken" in its view that notification was not required and held that it failed to notify individuals at he first reasonable opportunity:

> [81] Regarding the notification delay, the Custodian explained that, because the PHI in the employee's email account was primarily in non-consolidated and unidentifiable form, it took some time to identify the medical and treatment status for the affected individuals. Moreover, the Custodian explained that it (mistakenly)

took the view that notification was not required based on the Agent finding no evidence that the affected PHI was accessed, copied or exfiltrated.

[82] Although it may have taken the Custodian some time to identify which individuals were affected by the breach, in my view, once this determination was made in October 2020, these individuals should have received notification at that time. In my view, this would have been the first reasonable opportunity to do so, as the Custodian (and the Agent) did not provide any other evidence to suggest or demonstrate why notification could not have been provided to the affected individuals then.

Takeaway

Although this is not a reasoned IPC decision, its consequences are nonetheless significant. The IPC has taken the position that unauthorized access to an email account that holds personal health information is all that is necessary to trigger the duty to notify affected individuals. In turn, this requires health information custodians to conduct e-discovery on every compromised email account to identity who "may" have been affected and how. In our experience the cost of conducting such an analysis can range from $5,000 to $15,000. It also requires all affected patients to be notified that their personal information "may" have been browsed or downloaded – *i.e.*, "over notification." Such notification is costly, can lead to claims, and adds complexity to investigation and remediation efforts.

Proactively, health information custodian should revisit rules (and the enforcement of rules) relating to the sending and receiving of personal health information via email.

Should you have questions or if you are responding to a business email compromise, please contact any of the authors or key contacts listed below.

By

Daniel J. Michaluk

Expertise

Cybersecurity, Privacy & Data Protection, Health Law

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 725 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749

The information contained herein is of a general nature and is not intended to constitute legal advice, a complete statement of the law, or an opinion on any subject. No one should act upon it or refrain from acting without a thorough examination of the law after the facts of a specific situation are considered. You are urged to consult your legal adviser in cases of specific questions or concerns. BLG does not warrant or guarantee the accuracy, currency or completeness of this publication. No part of this publication may be reproduced without prior written permission of Borden Ladner Gervais LLP. If this publication was sent to you by BLG and you do not wish to receive further publications from BLG, you may ask to remove your contact information from our mailing lists by emailing unsubscribe@blg.com or manage your subscription preferences at blg.com/MyPreferences. If you feel you have received this message in error please contact communications@blg.com. BLG's privacy policy for publications may be found at blg.com/en/privacy.

© 2024 Borden Ladner Gervais LLP. Borden Ladner Gervais LLP is an Ontario Limited Liability Partnership.