Jennifer Johnson

From: Joseph Nilsson <jnilsson@idahofalls.gov>
Sent: Friday, September 18, 2026 9:09 AM
To: Consumer Protection Mailbox
Subject: Initial Breach Notification – City of Idaho Falls (Idaho Code § 28-51-105)

Attention: Corbin Schamber, Deputy Attorney General (208-334-4135)

Agency: City of Idaho Falls
Reported by: Joseph Nilsson, Chief Information Officer
Contact: jnilsson@idahofalls.gov, 208-612-8118

Summary of incident: On September 14, 2026, the Microsoft 365 mailbox of a City employee was accessed without authorization by an outside party using a stolen or replayed authentication token, from hosting infrastructure geolocated to Edison, NJ / Montreal, Canada (ASN associated with Tor/BitTorrent activity). The unauthorized session lasted approximately 60–75 seconds and involved automated access to roughly 70 items in the employee's Inbox, Sent Items, and Deleted Items folders, including repeated, targeted access to a folder containing archived payroll direct-deposit documentation.

An initial vendor-reported alert on this activity was closed on September 15, 2026 as a false positive based on an inaccurate secondhand explanation. A second, related alert on September 17, 2026 prompted a full technical investigation, which confirmed the unauthorized access was genuine. The City became aware that this constituted a confirmed breach of the security of the system on [September 17 / 18, 2026 — confirm exact date/time with City Attorney].

Personal information involved: Payroll and direct-deposit-related documentation belonging to one City employee, an Idaho resident. No evidence of file exfiltration from OneDrive/SharePoint, no persistence mechanisms (mail forwarding or inbox rules), and no unauthorized application access were identified. All outbound email from the account during the relevant window went only to internal City staff.

Number of Idaho residents affected: One (1).

Remediation to date: The affected account has been disabled, its password reset, all sessions and refresh tokens revoked, and MFA credentials reset and required to be re-registered. The City's policy requiring in-person verification for payroll direct-deposit changes substantially limits the practical risk of financial impact. The affected employee [has been / will be] notified directly so that he can verify his own account information and watch for suspicious contact.

Status: This investigation is complete as of September 18, 2026; a full internal incident report documenting the timeline, findings, and remediation is available to your office on request. The City is treating this as a confirmed compromise and is correcting the record with its security vendor accordingly.

Please let us know if the Attorney General's office requires any additional information.

Sincerely,

Joseph Nilsson | Chief Information Officer

308 Constitution Way
Idaho Falls, Idaho 83402
(208) 612-8118