04/06/26 12:06PM | Important Update from Truepoint Regarding Your Information

[redacted]

I am reaching out to make you aware of a recent cybersecurity incident. While I will be calling you very soon to discuss this and review any next steps, I first wanted to provide the background.

On Thursday, March 26, an unauthorized party temporarily gained access to a limited set of company files. Our team identified and eliminated the unauthorized access shortly after it was established.

We immediately launched a thorough investigation, with the assistance of trusted third-party forensic experts, to understand what occurred, what information may have been accessed, and whether there is any risk to you. We also began proactively monitoring client accounts for unusual activity and continue to do so. To date, we have not seen evidence of any fraudulent activity related to this incident.

The forensic review confirmed that only four files were downloaded, and those files were limited in content and contained no actionable information. Among the files that were accessed but not downloaded, a small number contained client information such as names, physical and email addresses, and account numbers—data comparable to what appears on a standard check. In your case, a file included your [redacted]

Although this information was not downloaded, there is no way to be certain it was not captured in some manner. Accordingly, we have enacted precautions to mitigate any potential risk. Importantly, even if this personal data is at risk, it would not be sufficient to enable unauthorized account access to your accounts. However, we recommend that you apply for a new passport and Truepoint will cover the cost and the cost for mailing the application. We can also help with the paperwork.

While our investigation was underway, we worked closely with our custodians to review account security and implement precautionary restrictions where appropriate. We continue to monitor accounts daily to help ensure account security and uninterrupted functioning.

We encourage you to remain attentive to your accounts and review notifications carefully. If you notice anything suspicious, please contact the financial institution and us immediately. As always, we strongly encourage the use of basic safeguards such as multi-factor authentication, strong passwords, and account alerts.

On behalf of our entire team, I apologize for this issue and the concern it may cause. We fully recognize the prevalence of cybercrime in today's world and remain committed to continually preparing our team and our clients to recognize and withstand these inevitable attacks. We take our responsibility to protect you very seriously and will do all we can to validate the trust and confidence you have placed in our firm through our response to this incident.