Key Facts about the Deloitte Email Cyber-Incident 6 October 2017

In response to a cyber-incident, Deloitte initiated a review to understand the scope of the incident, the potential impact to clients and other stakeholders, and to determine the appropriate cyber-security response. Below we share the key facts regarding this incident.

An attacker compromised account credentials and ultimately gained access to a single Deloitte cloud-based email platform. On discovering unauthorized access to the email platform, we initiated our standard and comprehensive incident response process, which included mobilizing a team of cyber-security and confidentiality experts inside and outside of Deloitte (including Mandiant). We engaged outside specialists to assure ourselves, clients, and other stakeholders that the review was thorough and objective. This team took a variety of actions:

- **Immediately executed steps to stop and contain the attack.**
- **Ascertained the size and scope of the attack.** The team reviewed logs from the incident to understand what the attacker did in the email platform, and it used this information to guide its response to the attack.
- **Determined what the attacker targeted.** The attacker targeted a cloud-based email platform. This system is distinct and separate from other Deloitte platforms, including those that host client data, collaborative work among Deloitte professionals, engagement systems and other non-cloud based email systems. None of these were impacted. We know from the forensic review conducted by our own cyber professionals, working alongside outside experts, that the attacker was specifically focused on obtaining active credentials.
- **Reviewed materials targeted by the hacker.** This incident involved unstructured data; namely, email. Through a detailed review of logs, Deloitte was able to determine what the attacker actually did and that the number of email messages targeted by the attacker was a small fraction of those stored on the platform. We looked at all of the targeted email messages in a manual document-by-document review process, with careful assessment of the nature of the information contained in each email. By conducting this eyes-on review, we were able to determine the very few instances where there may have been active credentials, personal information, or other sensitive information that had an impact on clients.
- **Contacted impacted clients.** Deloitte contacted each of these very few clients impacted.
- **Alerted authorities.** Deloitte began contacting governmental authorities immediately.
- **Took additional targeted steps to further enhance our overall security architecture.** We expanded our centrally controlled privileged access management system, and completed our roll out of multi-factor authentication (MFA), which was underway at the time of the attack. Now all users of the cloud-based email system and those with credentials with heightened access are part of our MFA system.

The team determined that:

- **The attacker is no longer in Deloitte's system**. Deloitte, with the assistance of outside experts, has seen no signs of any subsequent activities. We have taken a number of important steps to remove the attacker's access

to our environment, including the blocking of IP addresses, disabling accounts, resetting passwords, and implementing enhanced monitoring.
- **No disruption occurred to client businesses, to Deloitte's ability to serve clients, or to consumers.**

Our intensive and thorough review, which is complete, and our continued and significant investments in our cyber-security capabilities, reflect our commitment to protecting the information of Deloitte clients and stakeholders.