1. According to the interview with Dan in the article, “Sorry this fraud has been disconnected,” he:
   A. Started off nervous and was stammering.
   B. Wasn’t shocked that NyTell might have been defrauded.
   C. Said he didn’t think he could help the interviewer.
   D. Explained that he was the “go-to guy” for validating project invoices.

2. According to the article, “Sorry this fraud has been disconnected”:
   A. Dan never admitted that he knew the significance of his signature in the invoice-approval process.
   B. Despite his damaging admission, Dan insisted that TES was needed.
   C. Dan said he made the decision to engage additional ITC consultants.
   D. Dan immediately explained the specific services ITC provided.

3. According to the article, “Domains in disguise”:
   A. The scheme used a fake email domain intentionally designed to fool the recipient into thinking it came from his or her company.
   B. The banks, not the victim companies, suffered the full loss of the funds.
   C. In this fraud, a company’s shipping personnel receives an email from a supposed “middle manager.”
   D. The fraudsters requested that funds be wired to well-known “customers.”

4. According to the article, “Domains in disguise,” fraudsters in the scheme had access to the email inboxes, calendars and voice messaging systems of those responsible for transferring funds by wire.
   A. True.
   B. False.

5. According to the cover article interview, “Hacking the hackers,” Brian Krebs said:
   A. “Any organization connected to the Internet is vulnerable to immense data breaches.”
   B. “Threats to me and hacks on my websites are just some of the nuisances I have to endure.”
   C. “I’ve traveled to Russia several times to interview cybercriminals. Know thy enemy.”
   D. “Stolen credentials and passwords, in particular, are some of the most intractable problems in cybersecurity today.”

6. According to the cover article interview, “Hacking the hackers,” Brian Krebs said:
   A. “I have many contacts at banks who feed me information, and I supply them with my tips.”
   B. “Breaches often occur after fraudsters commit some fancy social engineering.”
   C. “Somehow, companies need to invest more in boots on the ground to help them effectively man all this security weaponry.”
   D. “Companies are vulnerable when they can manage Big Data.”

7. According to the article, “Botnets!”:
   A. Most of the cons originate in Pakistan, India and Jordan.
   B. Cybercriminals primarily use financial institutions to link up their botnets.
   C. Cybercriminals use their stolen money to set up drug and human trafficking rings in the Mideast.
   D. Once infected, a victim’s computer becomes part of the “C&C” infrastructure of a botnet.

8. According to the article, “Botnets!” most data breaches go unreported.
   A. True.
   B. False.

9. According to the article, “I didn’t intend to deceive anyone”:
   A. Someone who has intent to commit a crime acts with a deliberate, purposeful resolve — a desire to bring about a particular result.
   B. The three classifications of mens rea are intent, knowledge and desire.
   C. Anti-fraud pros might think “knowledge” is the only necessary state of mind.
   D. Classifications of mens rea do not vary among jurisdictions and laws.

10. According to the article, “I didn’t intend to deceive anyone”:
    A. Reckless conduct can even represent a medium deviation from a standard of care.
    B. The recklessness condition of mens rea doesn’t suffice to establish criminal culpability.
    C. Reckless conduct is when someone acts with a conscious disregard and exposes others to unjustifiable risk.
    D. The SEC’s complaint against Ebbers stated, “Ebbers didn’t know that WorldCom’s true method of accounting for line costs was not disclosed to WorldCom’s auditors.”