*Chapter 6*

**Criminal Law and Cyber Crime**

Answers to Learning Objectives/

Learning Objectives Check Questions

at the Beginning and the End of the Chapter

**Note that your students can find the answers to the even-numbered *Learning Objectives Check* questions in Appendix E at the end of the text. We repeat these answers here as a convenience to you.**

**1A.** ***What two elements normally must exist before a person can be held liable for a crime?*** Two elements must exist simultaneously for a person to be convicted of a crime: (1) the performance of a prohibited act and (2) a specified state of mind or intent on the part of the actor. A corporation may be held liable for crimes that their agents and employees commit within the course and scope of their employment.

**2A.** ***What are five broad categories of crimes? What is white-collar crime?*** Traditionally, crimes have been grouped into the following categories: violent crime (crimes against persons), property crime, public order crime, white-collar crime, and organized crime.

White-collar crime is an illegal act or series of acts committed by an individual or business entity using some nonviolent means usually in the course of a legitimate occupation.

**3A.** ***What defenses can be raised to avoid liability for criminal acts?*** Among the most defenses to criminal liability are infancy, intoxication, insan­ity, mistake, consent, duress, justifiable use of force, entrapment, the statute of limitations, and immunity.

**4A.** ***What constitutional safeguards exist to protect persons accused of crimes?*** Under the Fourth Amendment, before searching or seizing private property, law enforcement officers must obtain a search warrant, which requires probable cause.

Under the Fifth Amendment, no one can be deprived of “life, liberty, or property without due process of law.” The Fifth Amendment also protects persons against double jeopardy and self-incrimination.

The Sixth Amendment guarantees the right to a speedy trial, the right to a jury trial, the right to a public trial, the right to confront witnesses, and the right to counsel. Individuals who are arrested must be informed of cer­tain con­stitutional rights, including their Fifth Amendment right to remain silent and their Sixth Amendment right to counsel. All evi­dence obtained in violation of the Fourth, Fifth, and Sixth Amendments, as well as all evidence derived from the ille­gally ob­tained evidence, must be excluded from the trial.

The Eighth Amendment prohibits ex­cessive bail and fines, and cruel and unusual punishment.

**5A.** ***How has the Internet expanded opportunities for identity theft?*** The Internet provides easy access to private data. Web users surrender information about themselves without knowing it. Many Web sites use “cookies” to collect data on users who visit their sites. The data can include the areas of the site the user visits and the links on which the user clicks. Browsers often store information such as users’ names and e-mail addresses. Every time a purchase is made online, the item is linked to the purchaser’s name, allowing Web retailers to amass a database of who is buying what.

Answers to Critical Thinking Questions

**in the Features**

**Beyond Our Borders—Critical Thinking**

***Why might it be difficult for U.S. authorities to ever investigate the Koobface gang?*** The problem here is one of jurisdiction. The U.S. authorities have virtually no jurisdiction in Russia, and even if they did, it is well known that Russian officials would not cooperate.

**Adapting the Law to the Online Environment—Critical Thinking**

***What entities might pay “cyber mercenaries” to create some of the malware described in this feature?*** Of course, first and foremost would be governments that want to obtain diplomatic information or military secrets from other countries. Additionally, and perhaps increasingly, large business enterprises might wish to target other large business enterprises in other countries in order to steal intellectual property, such as trade secrets.

Answers to Critical Thinking Questions

**in the Cases**

Case 6.1—Critical Thinking—Social Consideration

***Who is in the best position to evaluate the credibility of the evidence and the witnesses in a case? Why?***In any case, the party in the best position to evaluate the credibility of the evidence and the witnesses is the factfinder who, at the trial level, is asked to make a determination with regard to the evidence. The factfinder in a trial is the jury, or in a non-jury case, the judge. This is because only the factfinder can be aware of the variations in demeanor and tone of voice that bear on the listener's understanding and belief in what is said.

In the *Smith* case, Smith waived his right to a jury trial so the judge was the factfinder. The trial court did not find Smith's testimony credible, determining that he “demonstrated a flexible approach to the truth—a looseness with the facts, in which the incriminatory truth is conceded only when and to the extent it is inescapable.”

Case 6.2—Critical Thinking—Legal Consideration

*Why was Sisuphan convicted of embezzlement instead of larceny? What is the difference between these two crimes?* One of the key differences between embezzlement and larceny has to do with the element of possession. Larceny involves the wrongful taking of property in the possession of another, as does robbery (the latter crime involves the violent taking of the property). Embezzlement, in contrast, involves the wrongful appropriation of property that has been entrusted to the person appropriating it, typically an employee. In other words, the property is already in the perpetrator’s possession.

Case 6.3—Critical Thinking—Technological Consideration

***If Miller and Marcum had used smartphones and U.S. Cellular had stored its records in the “cloud,” would the outcome likely have been different? Explain.*** No, if Miller and Marcum had used smartphones and U.S. Cellular had stored its records in the cloud, the outcome in this case would not likely have been different. The determining factor in cases involving cellphones and other electronic devices is the individual's decision to transmit a message to a device that could be in anybody's possession. This decision, and the transmittal and receipt, undercut the individual's expectation of privacy in that communication. The sending and receiving devices’ level of technological complexity is not controlling. For the same reason, the media used by the phone company to store the messages would not affect the result.

Answers to Questions in the Reviewing Feature

at the End of the Chapter

**1A.** ***State of mind***

Yes, because he was the corporate officer responsible for the project and had the power to prevent the criminal violation. Corporate directors and officers are personally liable for the crimes they commit, and can also be held liable for the crimes of employees under their supervision. Because Hanousek was the corporate officer responsible for every detail of the “6-mile” quarry, he had the power to prevent the criminal violation. Therefore, Hanousek can be held criminally negligent for the backhoe operator puncturing the pipeline.

**2A.** ***Theory of liability***

Under the responsible corporate officer doctrine, a corporate officer can be held liable for a crime because he was in a responsible relationship to the corpora­tion and could have prevented the violation. The corporate officer does not have to intend the crime or even know about it, to incur liability under this doctrine.

**3A.** ***Liability of employee***

No, because he did not have the required mental state (*mens rea)* and was not a cor­porate officer in a responsible position to prevent the criminal violation*.* Criminal liability requires a guilty act at the same time as the defendant had a wrongful mental state. In this situation, the backhoe operator did pierce the pipeline (the guilty act), but he did not have a wrongful mental state because he was unaware that the pipeline was there. As an employee, a court would not use the same standard as if he were a responsible corporate officer who “knew or should have known” of the existence of the pipeline. Because both elements of criminal liability (guilty act and wrongful mental state) did not occur, the backhoe operator could not be charged with a crime.

**4A.** ***Ignorance of the law***

No, because Hanousek was the corporate officer responsible for the project and should have known the requirements of the law. Because Hanousek was in a responsible position at the corporation and specifically in charge of the 6-mile quarry, a court would find that he “should have known” of the requirements of the law. Therefore, lack of knowledge of the requirements of the Clean Water Act would not operate as a defense in his case.

Answer to Debate This Question in the Reviewing Feature

at the End of the Chapter

***Because of overcriminalization, particularly by the federal government, Americans may be breaking the law regularly without knowing it.  Should Congress rescind many of the more than four thousand federal crimes now on the books?*** Difficult times require drastic measures.  This nation now has over 300 million residents who move frequently.  Moreover, the pervasiveness of the Internet means that business fraud is increasing at a rapid rate.  Consequently, the federal government must step in to make sure that criminal actions do not go unpunished.  That’s why so many new federal crimes have been added to the body of criminal statutes.

The Constitution reserves for the states police powers for activities within state boarders.  Crimes have always been defined by state and local governments.  Just because we have a larger population that has access to the Internet does not mean that Congress should be in the business of creating so many federal crimes.  Moreover, many new federal criminal statutes do not require intent—a cornerstone of the prosecution of most crimes for ages.

Answers to Issue Spotters

at the End of the Chapter

**1A.** ***Daisy takes her roommate’s credit card, intending to charge expenses that she incurs on a vacation. Her first stop is a gas station, where she uses the card to pay for gas. With respect to the gas station, has she com­mitted a crime? If so, what is it?*** Yes. With respect to the gas sta­tion, she has obtained goods by false pretenses. She might also be charged with larceny and forgery, and most states have spe­cial statutes covering illegal use of credit cards.

**2A.** ***Without permission,*** ***Ben downloads consumer credit files from a computer of Consumer Credit Agency. He then sells the data to Dawn. Has Ben committed a crime? If so, what is it?*** Yes. The Counterfeit Access Device and Computer Fraud and Abuse Act provides that a person who accesses a computer online, without permission, to obtain classified data—such as consumer credit files in a credit agency’s database—is subject to criminal prosecution. The crime has two elements: accessing the computer without permission and taking data. It is a felony if done for private financial gain. Penalties include fines and imprisonment for up to twenty years. The victim of the theft can also bring a civil suit against the criminal to obtain damages and other relief.

Answers to Questions and Case Problems

**at the End of the Chapter**

**Business Scenarios and Case Problems**

**6–1A.** ***Types of cyber crimes***

**1.** This is *vishing*, a form of identity theft. The traditional crimes of theft (rob­bery, burglary, larceny, and other) consist of wrongfully taking and carrying away an­other’s per­sonal property with the intent of depriving the owner permanently of it. Unique to crimes of identity theft is that they involve taking another’s identity, and unique to cyber variations of the offense is that the criminal acts are committed with computers, often online. A stolen identity is typically used to commit more crimes.

**2.** As in the previous problem, this is a form of identity theft. This problem de­scribes a factual situation referred to as *phishing*. In such a set of circumstances, once an unsuspecting individual responds by entering the requested information, the phisher can use it to pose as that person or to steal the funds in his or her bank or other account.

**3.** Here is identity theft in the form of *employment fraud*. In this scenario, the goal is to trick the recipient into revealing enough information for the perpetrator to steal his or her identity and commit still other offenses—emptying the individual’s ac­counts, spending money in his or her name, or otherwise taking advantage of his or her identity to obtain something undeserved or accomplish a criminal end.

**6–2A.  *Cyber scam***

Kayla has committed fraud in an e-mail sent via the Internet. The elements of the tort of fraud are as follows:

**1** The misrepresentation of material facts or conditions was made with knowledge that they were false or with reckless disregard for the truth.

**2.** There was an intent to induce another to rely on the misrepresentation.

**3.** There was justifiable reliance on the misrepresentation by the deceived party.

**4.** Damages were suffered as a result of the reliance.

**5.** There was a causal connection between the misrepresentation and the injury.

If any of Kayla’s recipients reply to her false plea with cash, it is likely that all of these requirements for fraud will have been met.

**6–3A. *Search***

Yes, a cross-gender strip search is unreasonable if there is no emergency—such as a riot or natural disaster—to justify it. Whether a search is reasonable under the Fourth Amendment requires balancing the need for the search against the invasion of personal rights that the search entails.

Here, there was no emergency situation, and there was no apparent justification for conducting a cross-gender strip search. In addition, the manner in which the search was conducted seems unreasonable. A female officer performed the search while several male officers watched, and one videotaped the search. There was no reason for the female officer to conduct the search immediately rather than another officer whose gender was the same as Byrd’s.

In the actual case on which this problem is based, the court held that the search performed on Byrd was unreasonable and violated Byrd's rights under the Fourth Amendment to be free from unreasonable searches.

**6–4A. *Credit- and debit-card theft***

Yes, there was sufficient evidence of credit- and debit-card theft for a court to uphold Turner’s conviction. Although there were no eyewitnesses to say they saw Turner take Barden’s purse, there was sufficient circumstantial evidence because Turner attempted to use Barden’s credit card immediately after the purse was taken. Turner also had Barden’s credit and debit cards on her at the time of her arrest. The appellate court refused to consider the credibility of Turner’s testimony that a friend had given her the credit and debit cards, because assessing credibility is the role of the trial court (and the jury, in jury trials). Turner had a long history of theft-related offenses and clearly knew that the credit and debit cards she had were stolen. Appellate courts focus on the law and evaluate whether the evidence was sufficient for conviction. In this situation, the appellate court found that the evidence was sufficient to uphold Turner’s convictions for theft. The court also upheld Turner’s sentence as a habitual offender because she had twelve prior felony convictions. She received a sentence of ten years in prison for theft of credit and debit cards—and a total of thirty years in prison when combined with additional charges.

**6–5A. Business Case Problem with Sample Answer—*Criminal liability***

Yes, Green exhibited the required mental state to establish criminal liability. A wrongful mental state (*mens rea*) is one of the elements typically required to establish criminal liability. The required mental state, or intent, is indicated in an applicable statute or law. For example, for murder, the required mental state is the intent to take another's life. A court can also find that the required mental state is present when a defendant’s acts are reckless or criminally negligent. A defendant is criminally reckless if he or she consciously disregards a substantial and unjustifiable risk.

In this problem, Green was clearly aware of the danger to which he was exposing people on the street below, but he did not indicate that he specifically intended to harm anyone. The risk of death created by his conduct, however, was obvious. He must have known what was likely to happen if a bottle or plate thrown from the height of twenty-six stories hit a pedestrian or the windshield of an occupied motor vehicle on the street below. Despite his claim that he was intoxicated, he was sufficiently aware to stop throwing things from the balcony when he saw police in the area, and he later recalled what he had done and what had happened.

In the actual case on which this problem is based, after a jury trial, Green was convicted of reckless endangerment. On appeal, a state intermediate appellate court affirmed the conviction, based in part on the reasoning stated above.

**6–6A. *White-collar crime***

Yes, the acts committed by Matthew Simpson and the others, and described in this problem, constitute wire and mail fraud. Federal law makes it a crime to devise any scheme that uses the U.S. mail, commercial carriers (FedEx, UPS), or wire (telegraph, telephone, television, the Internet, e-mail) with the intent to defraud the public.

Here, as stated in the facts, Simpson and his cohorts created and operated a series of corporate entities to defraud telecommunications companies, creditors, credit reporting agencies, and others. Through these entities, Simpson and the others used routing codes and spoofing services to make long distance calls appear to be local. They stole other firms’ network capacity and diverted payments to themselves. They leased goods and services without paying for them. And they assumed false identities, addresses, and credit histories, and issued false bills, invoices, financial statements, and credit references, in order to hide their association with their entities and with each other. The “scheme” was to defraud telecommunications companies and other members of the public to the perpetrators’ gain of a variety of goods and services. Wire services—the Internet, and presumably phones and other qualifying services—were used to further the scheme.

In the actual case on which this problem is based, a federal district court convicted Simpson of participating in a wire and mail fraud conspiracy (and other crimes). On appeal, the U.S. Court of Appeals for the Fifth Circuit affirmed the conviction.

**6–7A. *Defenses to criminal liability***

Yes, Barta could be absolved of the charge of conspiracy to commit bribery on a defense of entrapment. This defense is designed to prevent police officers and other government agents from enticing persons to commit crimes so that they can later be prosecuted for criminal acts. For entrapment to succeed as a defense, both the suggestion and the inducement to commit the crime must take place. The critical question is whether the person who is charged with the commission of a crime was predisposed to commit it or did so only because the officer induced it.

In this problem, the government, through its agent George Castro, entrapped Barta into participating in a conspiracy to bribe a fictional county official. The government conceded at Barta’s trial that he was not predisposed to conspire to commit bribery. Castro frequently e-mailed and called Barta over a period of months, with no response from him, even when the messages included deadlines and ultimatums. And Barta’s statement, when he eventually did write a check on his company’s account to Castro, that it was to help his friend gave the government reason to believe that Barta was making a deal only to benefit his friend.

In the actual case on which this problem is based, Barta was arrested, charged, and tried for conspiracy to commit bribery. He pleaded entrapment but was convicted. The U.S. Court of Appeals for the Seventh Circuit reversed his conviction, on the reasoning stated above.

**6–8A. A Question of Ethics—*Criminal process***

**1.** Peters can be perceived as an arrogant person—displaying a feeling of superiority—and lacking empathy for others, particularly those victims who trusted him and those whom he threatened. There is no indication that he had any sense of what it takes to live in society without lying to, stealing from, and victimizing others. To behave ethically requires at least a willingness to refrain from illegal conduct and a degree of empathy for others. Peters’s misconduct showed that his character lacked these qualities. In other words, he seems to have had no ethical principles.

It might be pointed out that if Peters had put the ingenuity and energy he expended on his illegal schemes to legal, practical use, he might have engineered a successful business. Instead, his lack of ethics robbed himself and others of money and property, as well as the opportunity to trust and be trusted and to do business in good faith.

**2.** The court that sentenced Peters concluded that a sentence of forty-eight months imprisonment was appropriate. The court found the federal sentencing guidelines “entirely inadequate in this case. They fail to account for the threats that were made to the victim and his wife. They fail to account for the kinds of vulnerabilities that someone in this victim's situation faced. The guidelines are too low in this case in relationship to the defendant's criminal history and the defendant's conduct. . . . His own family describes him as a thief.”

The U.S. Court of Appeals for the Eleventh Circuit affirmed the sentence. “An above-guideline range sentence was necessary to achieve the statutory purposes of sentencing. As the court found, the conduct underlying the offense was serious.” Peters's criminal history supported a need for “deterrence in fashioning an appropriate sentence. The sentence is also supported by the need to protect the public from further crimes of Peters.” The court added, “The 48–month sentence was considerably lower than the statutory maximum sentence of 20 years, signaling that the sentence was substantively reasonable.”

**Critical Thinking and Writing Assignments**

**6–9A. Critical Legal Thinking**

The answer to this question is no. A separate crime occurs only when there are separate distinct acts of seizing the property of another. In the circumstances described in the question, Ray committed the crime of grand theft because of the value of property in the purse, including the value of the gun. Only one crime of theft occurred, however. Ray saw the purse and took it without know­ing what it contained: there was one intent and one act.

**6–10A. Business Law Critical Thinking Group Assignment**

**1.** It goes without saying that the higher the anticipated cost of engaging in cyber crime activity, the lower will be the amount demanded.  In other words, heavy fines and long jail sentences would have some deterrent effect.  The real question is by how much.  Many hackers who bring down corporate and government computer systems are teenagers.  They cost businesses billions of dollars, yet gain no monetary reward for their hacking—they do it to prove that they are as good or better than other hackers.  If caught, they could not engage in much meaningful restitution to their corporate victims.  In contrast, adult cyber criminals who engage in identity theft, credit-card fraud, and online auction fraud often make larges sums of money from this criminal activity.  They could be forced to engage in meaningful restitution to their victims.  They could be sentenced to long jail terms, just as we routinely do for traditional thieves.  Restitution and long jail terms might serve as a deterrent to such cyber criminal activities.  U.S. authorities, though, cannot easily arrest, try, convict, and sentence cyber criminals living and operating in, say, Russia.

**2.** Protection against cyber crime starts with the awareness at management and staff levels of the potential harm that could result. Even the temporary loss of a system’s functions while its software is replaced due to a virus’s infection or other destructive event could prove costly. Thus, management should make appropriate funds available to pay for security, impose procedures to identify the system’s vulnerability, require the use of security hardware and software, and conduct security audits on an ongoing basis. The use of passwords among those with access to the system is also an important step when used correctly. Backed-up data can be key, and storing the backed-up data off-site can be even more effective.