A1. CFAA and ECPA

The Computer Fraud and Abuse Act (CFAA) is violated when a protected computer is accessed without authorization, leading to fraudulent activities or damage. In the TechFite case study, unapproved accounts were created by Carl Jaspers, which were then used to perform intelligence-gathering activities against various companies. These accounts remained active despite the employees assigned to them having left the company over a year ago. Emails linked to these accounts contained references to intelligence-gathering tactics such as dumpster diving against multiple businesses. Additionally, evidence of penetration and scanning activities targeting several internet-based companies using the Metasploit tool was found on multiple devices within the Business Intelligence (BI) Unit. These activities demonstrate unauthorized access and system exploitation, violating the CFAA.

The Electronic Communications Privacy Act (ECPA) prohibits unauthorized access, interception, and disclosure of Electronic Communications. In the case study, the BI unit used dummy accounts to penetrate internal TechFite departments (legal, HR, and Finance) and gain access to executive and financial documents without authorization. Networking logs revealed that BI Unit employees, including Sarah Miller, Megan Rogers, and Jack Hudson, accessed these internal documents regularly. This evidence shows that private company information was accessed and passed on to competitors. Unauthorized disclosure and interception of electronic communications violates the ECPA.

A2. Three Laws

An example of carelessness in facilitating an ECPA violation was the lack of internal control over user accounts and data access. No policies or procedures were in place to prevent prohibited privilege escalation, which allowed Sarah Miller and her team access to confidential financial and executive records. This carelessness enables unauthorized disclosure of electronic communications, which justifies legal action under the ECPA.

The failure to monitor user accounts and prevent illegitimate use was a similar case of negligence that resulted in a CFAA violation. These fraudulent accounts, which Carl Jaspers kept active, enabled system exploitation. The IT department, specifically IT Analyst Nadia Johnson, failed to audit or flag these suspicious accounts, further exacerbating the security lapse. The lack of internal auditing and enforcement of cybersecurity protocols allowed unapproved access, which gave rise to CFAA legal action.

Negligence was also observed in violations of the Sarbanes-Oxley Act (SOX), which mandates financial transparency and accountability. The existence of three companies, Bebop Software, FGH Research Grough, and Dazzling Comet Software, suggests financial fraud. These entities had no legitimate online presence but funneled money through FreeWorkers' Pennsylvania Bank, which TechFite does not do business with. These payments were likely arranged by Carl Jaspers and his former Stanford associate, Yu Lee, the registered agent for all three companies. The absence of proper financial oversight and internal auditing enabled financial misconduct. Justifying legal action under SOX.

A3. Duty of Due Care

The first failure in the duty of due care is the lack of security measures to prevent unauthorized data access and unauthorized use. TechFite did not enforce least privilege principles or separation of duties within the BI unit, allowing unrestricted access to sensitive client information. Internal monitoring tools failed to detect that Sarah Miller and her team were actively scanning other companies' networks. This failure led to competitors acquiring proprietary data that was likely used to launch similar products, causing financial harm to affected businesses.

A second failure was the lack of oversight in financial transactions. TechFite's finance department failed to scrutinize payments from questionable entities linked to Carl Jaspers and Yu Lee, enabling potential money laundering or fraudulent financial reporting. Despite the unusual pattern of payments all coming from the same bank, Free Workers' Pennsylvania Bank, no red flags were raised. The absence of internal controls encouraged unethical business practices and indicated a serious lack of due diligence and corporate responsibility.

A4. SOX

As a publicly traded company on NASDAQ, TechFite is subject to the Sarbanes Oxley Act, which requires fiscal transparency and accountability. The fraudulent financial activities tied to the BI Unit, including payments from questionable entities and possible sales figure inflation, are a violation of SOX. The lack of financial controls and audits allowed these practices to continue unchecked, violating SOX regulations.

B1/B1a. Criminal Evidence, Activity, Actors, and Victims

A clear criminal act in the case study is the unwarranted access and leaking of proprietary data from potential clients Orange Leaf Software and Union City Electronic Ventures. The principal perpetrators were Carl Jaspers, Sarrah Miller, Megan Rogers, and Jack Hudson, who misused information derived from consulting discussions. Victims of the act included

Orange Leaf Software and Union City Electronic Ventures, whose competitive advantage was eroded when rivals launched similar products.

A second crime is the possible financial fraud involving the three questionable companies, Bebop Software, FGH Research Group, and Dazzling Comet Software. These entities made payments through an unrelated bank and may have been trying to manipulate TechFite's financial records. The mastermind behind this scheme appears to be Carl Jaspers, working with Yu Lee. TechFite's shareholders and regulatory bodies are the primary victims of this financial misconduct.

B1b. Cybersecurity Policies & Procedures for Criminal Activity

A Data Loss Prevention (DLP) policy could have prevented the unauthorized leak of proprietary client information. Strict controls on the movement of sensitive data and monitoring internal transfers could have prevented a data leak from occurring.

A Financial Transactions Monitoring policy might have flagged the irregularities in payments from the questionable entities linked to Carl Jaspers and Yu Lee. Automated financial auditing and transaction verifications would have flagged suspicious banking activities and prevented fraudulent transactions.

B2/B2a. Evidence of Negligent Activity, Actors, and Victims

An example of negligence is the failure to audit user accounts internally. IT Security Analyst Nadia Johnson failed to deactivate the accounts of former employees, which were exploited by Jasper and his team. TechFite's clients, such as Orange Leaf Software and Union City Electronic Ventures, were the primary victims.

Another example of negligence is the oversight of financial transactions. The finance team was unable to spot fraudulent payments from unconfirmed sources, allowing financial misconduct. This failure in financial governance affected shareholders and regulatory authorities.

B2b. Cybersecurity Policies & Procedures for Negligent Activity

A User Access Review policy could have prevented unofficial account use by deactivating inactive or unnecessary accounts. Periodic audit of user accounts would have found and removed fraudulent access.

A Segregation of Duties policy in financial management could have prevented unchecked financial transactions by ensuring that no single employee has complete control over creating, recording, and verifying transactions.

C. Legal Compliance Summary for Management

TechFite is currently non-compliant with several cybersecurity and financial regulations. Unauthorized system access and intelligence-gathering activities reflect violations of the CFAA. The company has not enforced user account auditing and privilege restrictions, allowing for unauthorized intrusions. ECPA compliance also suffers from internal data leaks, such as Sarah Miller, Megan Rogers, and Jack Hudson's interception of confidential communications. The company has no clear policies to prevent or monitor such activities.

TechFite is also non-compliant with SOX on account of financial misconduct. Irregular financial transactions and potential revenue inflation point to violations of financial reporting standards. The company's financial team failed to detect unusual transactions involving Bebop Software, FGH, and Dazzling Comet Software, which may have been shell companies. Urgent corrective actions, including tightening cybersecurity policies and strengthening financial oversight, are required to curtail legal risks and prevent future regulatory breaches.