PacificCPE

COURSE
11802A

Cybercrime and Digital Fraud Investigations

Digital technology has transformed how fraud is committed, and forensic accountants must evolve alongside it. This chapter explores cybercrime as it intersects with financial fraud, covering how criminals exploit digital systems and what that means for investigations. CPAs and financial professionals will gain a practical understanding of the digital landscape, learn how electronic evidence fits into fraud cases, and build awareness of the tools and techniques used to uncover financially motivated cybercrime in today's connected environment.

CREDIT HOURS 2 | FIELD OF STUDY AUDITING | EXAM QUESTIONS 10

Start Course ↓ | Final Exam Copy ↓

Assignment

- Study the full course materials included here.
- Complete the review questions after each chapter.
- Answer 10 final exam questions.
- Final exam is scored immediately, 70% or better passes.
- Certificate of completion is available in your account.
- Failed exams can be retaken free of charge.

Course Objectives

- Recall the characteristics of various computer-related crimes.

Copyright Notice

© 2026 Pacific CPE, LP. All rights reserved.

This course and test have been adapted from supplemental materials and uses partial text from the materials entitled Forensic Accounting and Fraud Examination, 3rd Edition by Mary-Jo Kranacher and Richard A. Riley, Jr. © 2024 by John Wiley & Sons, Inc. Displayed by permission of the publisher, John Wiley & Sons, Inc., Hoboken, New Jersey.

The materials in this course — including the text, illustrations, exhibits, examples, exam questions, and review questions — are the copyrighted property of Pacific CPE, LP. No portion of this course may be reproduced, stored in a retrieval system, distributed, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise) without the prior written permission of Pacific CPE, LP, except for the personal, non-commercial use of the registered learner.

Pacific CPE, LP grants the registered learner a single-seat, non-transferable license to access this course for the purpose of completing the associated continuing professional education credit. Account credentials may not be shared.

This course is provided "as is" for educational purposes. While Pacific CPE, LP makes a reasonable effort to ensure the content is current and accurate, the materials should not be relied upon as a substitute for professional advice. Pacific CPE, LP disclaims all liability for any error, omission, or loss arising from the use of, or reliance on, the course content.

Publication Date: August 2026

TABLE OF CONTENTS

CHAPTER 01

Cybercrime: Fraud In A Digital World 4

1.01 Module 1: The Digital Environment 6

1.02 Module 2: Frauds And Other Threats In The Digital World 18

1.03 Module 3: Cyber Fraud 33

1.04 Module 4: Complex Frauds And Financial Crimes In Cyberspace 40

1.05 Module 5: Reporting Cybercrime 46

Test Your Knowledge 49

Final Exam Copy 71

Glossary 59

Index .....

Chapter 1: CYBERCRIME: FRAUD IN A DIGITAL WORLD

Chapter Objective

After completing this chapter, you should be able to:

- Recall the characteristics of various computer-related crimes.

According to Justice News: FTX Founder Indicted for Fraud, Money Laundering, and Campaign Finance Offenses [1]

> *A federal grand jury in Manhattan returned an indictment today charging Samuel Bankman-Fried, aka SBF, 30, of Stanford, California, with wire fraud, conspiracy to commit wire fraud, conspiracy to commit commodities fraud, conspiracy to commit securities fraud, conspiracy to commit money laundering, and conspiracy to defraud the Federal Election Commission and commit campaign finance violations.*
>
> *The charges in the indictment arise from an alleged wide-ranging scheme by Bankman- Fried to misappropriate billions of dollars of customer funds deposited with FTX—the international cryptocurrency exchange founded by Bankman-Fried—and mislead investors and lenders to FTX and Alameda Research, the cryptocurrency hedge fund also founded by Bankman-Fried. He was arrested yesterday in the Bahamas on these charges and will be presented before a Bahamian magistrate judge today.*

According to reporters at NPR and Reuters, Bankman-Fried was taken into custody in the Bahamas at the request of the U.S. government. FTX, formerly a major player in virtual currencies, had filed for bankruptcy in November 2022. Evidence suggested that FTX was insolvent and illegally moving money. Bankman-Fried resigned hours before the bankruptcy filing but claimed innocence of any wrongdoing. [2]

Cryptocurrencies are an electronic money movement and payment system. While available since at least 2009, cryptocurrencies, led by huge increases in value, really broke into the eye of the public in 2017. The 2017 cryptocurrency movement was grounded in ICOs (Initial Coin Offerings). ICOs are a means of funding a business venture by issuing a cryptocurrency rather than traditional angel, venture, or some other form of investment capital.

In general, the investment process is as follows: the cryptocurrency is issued to the investor and the issuer collects cash for operations and investment. Such an approach to raising money allows the issuer to avoid regulations and the processes required to register investments. In 2017, ICOs went from being a relatively unknown fundraising method used in the blockchain community, to raising

over $4 billion. Because investors hold currency rather than ownership shares, the issuer has little (legal) obligations to those receiving the cryptocurrency. [3]

Jordan Underhill, ACFE Research Specialist, J.D., CFE, likens some of the smaller cryptocurrency offerings to being similar to "penny stocks." As such, they are subject to abuse via schemes similar to pump and dump. While the funded organization gets its cash flow, the holders of the cryptocurrency are left with little to no legal protection. According to Underhill, forensic accountants and fraud examiners need to have some sense of how cryptocurrencies and ICOs work. Underhill suggests that rather than the professional perceiving cryptocurrency as a new scheme, it is better understood as a new tool to perpetrate old schemes.

Over time, blockchain, the technology underlying Bitcoin and other cryptocurrencies, could potentially have many uses and may even help to prevent fraud by better tracking the flow of money. As such, antifraud and forensic accounting professionals should expect to encounter them during their career. [4]

The role of technology as it relates to fraud, financial crime, and other bad acts can seem a bit overwhelming. At the same time, technology offers additional tools such as big data, financial analytics, robotic process automation, and artificial intelligence that can facilitate efficient and effective prevention, detection, and deterrence. Further, it is important for FAFE professionals to understand current technology, cyber threats, and antifraud efforts in this complex and dynamic space.

In this chapter, we examine these topics across several modules. Those modules, along with the learning objectives, include the following:

- Module 1 provides an overview of the digital environment, including the availability and trends to switch to a currency-less society. The objective for Module 1 is for readers to understand and articulate the many threats in the digital environment; the goal is for readers to better prevent, deter, and detect bad acts in the digital world.
- Module 2 dives deeper into the types of threats, including fraud, that participants, who embrace digital activities (such as social media, e- and m-commerce and other new technologies), may face. The goal of Module 2 is for readers to be aware of, and alert for, potential threats encountered as digital citizens.
- Module 3 examines cyberfraud. The learning outcomes for Module 3 include the ability to identify major categories of cyberfraud and evaluate organizational and individual risks.
- Module 4 considers complex fraud and financial crimes in cyberspace. Complex fraud often involves collusion and offenses in multiple jurisdictions. The objective of Module 4 is for the reader to examine cyberfraud and other financial crimes, such as money laundering, in a complex and international context.

- Module 5 reviews one of the primary means of reporting cyberfraud and other digitally based crimes. In some cases, local law enforcement may not have the requisite knowledge, skills and abilities, or the jurisdiction, to effectively and efficiently examine bad acts in a digital environment. In the United States, the Internet Crime Complaint Center (I3C), among other federal agencies, may be the best point of contact for information and reporting. The goal of Module 5 is for readers to identify resources when facing cyber threats and incidents.

MODULE 1: THE DIGITAL ENVIRONMENT

Nick Tranto, Headquarters Excise Tax Policy Manager for the Internal Revenue Service (retired), describes three eras of fraudulent activity. He refers to the first era as the "Paleolithic Era." In this era, fraudulent criminal activity centered on cash, laundering cash, and evading taxes. Organized criminal activities and creative fraud schemes also usually involved other illegal activities, such as alcohol, gambling, prostitution, guns, and drugs. These activities became large scale in the 1920s and 1930s due to prohibition of the distribution and sale of alcoholic beverages. Many were orchestrated by individuals ranging from smalltime thugs to "the mob" and invoke images of Al Capone and Hollywood characters, such as those in *The Godfather*, *Goodfellas*, and *The Untouchables*. The primary problem was the need to handle large amounts of cash generated from the illicit and illegal activities, as well as bribes and kickbacks to keep elected officials and law enforcement from scrutinizing the activities too carefully. Some of the early and more creative money laundering schemes were developed during this time and a fundamental goal was to evade taxes.

The second major era started in the 1960s, and Tranto describes this period as the "Neolithic Era" of organized criminal operations and the sophisticated predator fraudster. At this point in time, bad actors discovered that "an accountant with a sharp pencil could steal more than twenty criminals armed with guns." Many of the perpetrators were first-generation college graduates and sons of mobsters (SMOB). Tax evasion and money laundering continued to be the major focus of the organized criminal activities. The structure, however, included more traditional organizational forms, such as legitimate casino businesses, other cash-heavy businesses, and the interaction between legitimate and illegitimate business activities. The proceeds from these activities could be concealed and then made available for the perpetrators to use openly because of seemingly legitimate business fronts. This arrangement was, to some degree, a reaction by the bad actors to more sophisticated law enforcement investigation methods, improvements in the judicial system, and a greater intolerance by society for blatant deviant behavior. These changes put pressure on individuals with bad intentions to better conceal their illegal activities so they could fit into society as "upstanding citizens."

Mr. Tranto describes the third period as the "Geek-olithic Era." In the third era, cash generated from illegal activities is still a primary problem. But in the Geek-olithic era, smart individuals with

questionable ethics became significant fraud perpetrators. The bad actors now include computer specialists, attorneys, MBAs, Wall Street professionals, and others who use tools and techniques, such as offshore bank accounts, Internet servers, jurisdictional barriers to enforcement, and technology to move and hide billions of dollars. Once money appears to be legitimate (laundered), it is then able to be moved and used, as if it came from legitimate sources. In addition, more creative fraud schemes were created, and the use of technology often became integral to the act, the concealment, and the conversion. In the Geek- olithic era, investigators need to use digital tools and techniques for data extraction and analysis to catch the crooks. The complexity of the schemes often demands the ability to connect seemingly disparate activities and financial transactions to businesses and organizations located around the world. Without technological resources, the investigator's effectiveness can be greatly diminished. In short, because the bad actors have made computers integral to their crimes, investigators need to arm themselves with the same tools to level the playing field.

Assume, for example, that a drug dealer on a neighborhood street corner hands over drugs to a customer and the customer pays for the contraband by "zapping" money from his Internet-connected cell phone to the dealer's cell phone. The police observe the transaction and approach the dealer. The dealer, perceiving the approach of the police, ejects a memory card from his phone and drops the useless cell phone in the closest sewer, tucking the tiny memory card into his pocket. By the time the police grab the suspect, all evidence is gone except for a tiny memory card that the police have confiscated but have no idea what it contains and cannot access it because of encryption. The Geek-olithic perpetrator—from the small-time but electronically savvy neighborhood to the well-organized, international Internet scammer— presents new and challenging problems for law enforcement and other investigators. In our tech-savvy world, data exists in many forms and places, but it requires a targeted approach and an embrace of technologically based investigative solutions.

Cybercrime, in the "Geek-olithic Era," usually describes criminal activities in which a computer or network of computers is an integral part of the crime. Examples include spamming, theft of electronic intellectual property, unauthorized access (e.g., defeating access controls), malicious code (e.g., computer viruses), denial-of-service attacks, theft of service (e.g., telecom fraud), and computer-based investment and other financial frauds. Some cybercrime, such as the Nigerian cash transfer e-mails and other e-mail scams, are grounded in the gullibility (social engineering) of the victim. Other cybercrimes include hacking, "phishing," identity theft, child pornography, online gambling, securities fraud, cyberstalking, theft of trade secrets, and industrial or economic espionage. Some cybercrimes, such as "information warfare," have national security implications. Thus, cybercrime includes a blend of traditional crimes and newer derivations in which computers or networks are used to facilitate, conceal, and generate benefits to the perpetrator of the illicit activity.

As an example of the use of cyberspace to advance nefarious activities, according to *Gangbangers Invade Cyberspace*, by Steve Macko, ENN Editor, cyberspace is now

> *a place for gang members to exchange ideas on how to improve drug sales, what's the best gun to use to shoot your business rivals and what are the best drugs to use in your spare time? ... all of that and more can be found on the Glock3 website. This site is said to link members of street gangs from around the world, from 'Lil Shorty's Click in London to the Gangster Disciples in Chicago to the West Side Crips in Phoenix. Experts say that the site provides a virtual "how-to" for wannabe street gang members.*

Another way to describe cybercrime is criminal activity involving information technology infrastructure, including unauthorized asset destruction, file and software deletion, service attacks that result in deterioration, alteration, or suppression of computer data, and unauthorized use of devices. Personal computers, computer systems and digital devices that capture and process electronic data are powerful, small, inexpensive, and user-friendly. As computers and digital technology have advanced, electronic devices have proliferated in society, businesses, and in our everyday lives. Modern business, government, and other organizations, including criminal enterprises, depend on computer systems to support their operations.

Initially, transactions captured and processed by computer systems had hard copy supporting documentation. In the absence or destruction of computer storage where data was damaged, transactions could be reconstructed from physical forms and documents. In today's environment, the computer is integrally embedded in most business and government processes and less hard copy backup exists. Computers have invaded almost every aspect of our lives, including tax return processing, electronic calendars and contact lists, cooking recipes, robotics, budgeting, automobile operations, weapons systems, law enforcement systems, and automated teller machines (ATM). More and more people around the globe rely on computers and digital devices in their everyday lives. As businesses, government agencies, and individuals become increasingly dependent on digital devices, so do those with criminal intentions. Individual criminals and criminal enterprises use computers to support their illegal operations for everything from facilitating the movement of cash around the world to real-time communications through e-mail, text messaging, and disposable cell phones. Cybercrime and computer and Internet frauds are increasing in frequency and size, and this trend is likely to continue. More computers, and thus criminals, are networked internationally, giving global access to cybercriminals.

The Role of Digital Devices in Cybercrime

Computer crime is an illegal offense that is committed where the computer or electronic data device is integral to the criminal act. In this context, "computer" has a broad definition and can mean personal computer, notebook, tablet, iPad, smartphone, or any other digital device that has software installed. Consider the Internet of Things (IoT): Even home appliances, HVAC controls, and other

smart home devices have software and computer-like characteristics and can be operationalized for bad acts. The computer, no matter how it is defined, has several roles in high-tech crime, both as a tool and a target. According to Donn B. Parker, a cybercrime authority and author, the function of the computer in crime is fourfold, as an object, a subject, a tool, and a symbol.

- The Computer as an Object—Computers and network systems are themselves often objects or targets of crime, subject to physical sabotage, theft, or destruction of information.
- The Computer as a Subject—Computers can be the direct subjects of crime when technologists use the computer to commit a crime. This category includes virus attacks, illegal access, etc.
- The Computer as a Tool—Computers can be integral to the act, the concealment, and the conversion associated with a fraud or financial crime when the electronic device is used to commit a crime, whether embezzlement, theft of proprietary information, or hacking.
- The Computer as a Symbol—Computers lend fraudsters an air of credibility and are often used to deceive victims into investment, pyramid, and other "traditional" fraud schemes that have been adapted to the digital environment.

Some common examples of computer crimes include:

- Data alteration
- Unauthorized access and entry to systems and information
- Reading another's e-mail without permission
- Data destruction and sabotage
- Internet consumer fraud
- Sale of proprietary data
- Desktop counterfeiting
- Data extortion
- Disclosure of confidential data
- Identity theft
- Electronic letter bombing
- Software piracy
- Voice mail fraud
- Cellular telephone fraud

Computer Fraud versus Computer Crime

Two terms that are commonly used interchangeably are computer fraud (and financial crimes) and computer crime, yet substantial differences exist between them. First, computer-based fraud and financial crimes are any defalcation, fraud, or financial crime accomplished by tampering with

computer programs, data files, operations, equipment, or media, and result in losses sustained by the organization whose computer system was compromised. One of the distinguishing characteristics of computer-based fraud is that access occurs with the intent to execute a fraudulent scheme or financial criminal act.

In short, most jurisdictions have defined computer fraud as an "attempt crime." By viewing the computer as a protected asset, the protection is independent of the actual loss to the owner as a result of the intrusion.

In contrast to computer fraud, computer crime is defined as an act where the computer hardware, software, or data is altered, destroyed, manipulated, or compromised due to acts that are not intended. Generally, computer crime differs from computer fraud in at least three major ways:

1. Employees who, as a part of their assigned duties and responsibilities, have access to the computer systems are deemed to have authorized access. As a result, those with authorized access cannot fall under statutes that address computer fraud (outlawing unauthorized access), even if their actions subsequent to access are judged illegal. Individuals with some authorized access but who exceeded that authorization can be prosecuted under computer-based fraud statutes. Thus, "without authorization" generally refers to intrusions by outsiders or those with no access, but some courts have also applied the term to intrusions by insiders who access computers other than the computer they are authorized to use, intrusions by insiders acting as agents for outsiders, and intrusions by insiders who violate clearly defined access policies.
2. The manipulation, alteration, or destruction of data (including computer software) is considered independent of computer-based fraudulent schemes.
3. Because data are intangible, the destruction or compromising of the integrity of computer data does not fall under vandalism statutes.

As a result of the preceding discussion, computer-based fraud and financial crimes are technically not "computer crimes" but often involve the use of computers as a means to break the law. In some cases, traditionally illegal acts can yield more ill-gotten gains by utilizing the speed, power, and global access of computers, other digital devices, and their users. A more apt term may be computer-assisted crimes. In such cases where traditional frauds and financial crimes are facilitated through the incorporation of electronic devices, existing criminal laws can be applied to the acts. The main benefit of the computer fraud and computer crime statutes, however, is derived when proving traditional crimes is difficult because the evidence of such acts have been destroyed electronically. In such cases, computer fraud and computer crime laws are invaluable as an alternative method of prosecution.

Historically, in the early 1980s, law enforcement agencies faced the dawn of the computer age with growing concern about the lack of criminal laws available to fight emerging computer crimes.