OHANA GROWTH PARTNERS, LLC	**IN THE**
Plaintiff,	**CIRCUIT COURT**
vs.	**FOR**
RYAN DILLON-CAPPS	**BALTIMORE COUNTY**
Defendant.	**CASE NO: C-03-CV-24-002264**

AFFIDAVIT OF LEGAL OBLIGATIONS

I, Ryan Dillon-Capps, being over the age of eighteen (18) and competent to testify, and having personal knowledge of the facts contained herein; provide the following statement of facts and statements as follows:

Table of Contents

I BACKGROUND

A IT Department

1 Ryan Dillon-Capps joined Ohana Growth Partners in 2020 as part of a two-person IT department, alongside the Director of Business Intelligence, with several third-party vendors providing support. Baltimore Consulting (BC), led by Ryan Brooks, was brought in to handle system and cloud administration. Brooks took care of more advanced tasks, while BC employees handled routine office support, such as maintaining printers and conference rooms.

2 Dillon-Capps was quickly recognized as a valuable resource and welcomed as a key addition to the executive team. In 2021, they took on the role of PCI Compliance Officer, further

expanding their responsibilities. Over the following years, Dillon-Capps continued to take on more duties and was given increasing opportunities, leading to discussions in 2023 about a forthcoming C-level promotion. Prior to October 16, 2023, they were negotiating compensation packages in preparation for this promotion.

3 In addition to Brooks' role, he also developed solutions such as the company's intranet, which enabled employees to submit expenses, request reimbursements, and approve invoices. He also developed the iPad Kiosk platform, centralizing management of the landing page for prospects and members to enter payment information.

4 Marc Radic, owner of Fused Technologies, provided primary communication and network engineering support, with backup from Brooks. Radic also handled IT and entertainment installation and on-site support for Maryland-based Planet Fitness and Brick Bodies gyms.

5 Cielo IT initially provided Help Desk support, evolving over time to manage the Microsoft Cloud environment. They became the central point for addressing user and gym support needs, even those beyond their immediate responsibilities.

6 Logically, previously known as Cerdant, remained a mandated vendor for Planet Fitness franchisees, providing Security Operation Center (SOC) services, including managing the Point of Sale (POS) switch and firewall as part of the franchise agreements with Planet Fitness headquarters.

B Franchise Compliance

7 The franchisor and the processor require franchisees to sign both federal and state-regulated Franchise Disclosure Documents (FDD) and an addendum to the processor’s Master

Service Agreement (MSA). These agreements create a chain of duties, obligations, and liabilities extending from credit card companies, banks, and processors, down to merchants and franchisees, including PCI DSS compliance requirements.

8 Ohana Growth Partners operates Planet Fitness locations under franchise agreements but does not own the Planet Fitness brand beyond the conditions laid out in the Franchise Disclosure Document, the Area Development Agreement (PF-ADA), and other agreements with Planet Fitness Headquarters (PFHQ). PFHQ has exercised its ownership rights by determining terms that impact the rights of gyms, including compensation for the transfer of limited rights from one party to another.

9 PFHQ retains the ability to mandate terms and conditions as specified in the franchise agreement. These mandates can result in companies no longer being allowed to operate Planet Fitness gyms or profit from them if contractual obligations are not met.

10 Ohana Growth Partners may be exposed to liabilities due to PCI compliance issues. This could place both PFHQ and Ohana at legal risk, including potential breaches of contractual obligations. Additionally, compliance requirements might have been violated in several other states. Any incident relating to personal information protection, consumer credit reporting, computer crime, or securities laws could have significant legal and financial consequences for Ohana Growth Partners, LLC.

C Negligent Risk to Public Safety

11 The Plaintiff's civil lawsuit portrays events that are entirely fictional, falsely claiming ownership of Planet Fitness gyms that they can operate without adherence to contractual

obligation that mandates PCI Compliance. Ignoring years of adhering to Dillon-Capps decisions on the application of PCI DSS Regulations and forgetting over a dozen contractual obligations that mandate compliance as a top priority that has never been matched as to cause question about the supremacy of maintaining PCI Compliance because failure could result in the loss of the franchise and payment processing rights which would be a catastrophic event that may be ruinous. In every state that Ohana operates in they will sign a jointly regulated by federal and state authorities Franchise Disclosure Document (FDD). am providing sections of a copy of the 2024 FDD so the court can see this is a combination of agreements that include unique contracts as well as modifications to other agreements that they will have also signed and can provide the entire clean copy upon request. Since the question of access pertained to the centralized system affecting all locations. The violation would breach every FDD that the Plaintiff signed, specifically violating sections related to compliance with PCI DSS requirements.

12 Every FDD contains an addendum to the Master Service Agreement (MSA) because the processor for all of Planet **Fitness** is a Payment Service Provider (PSP). Most processors require lengthy contractual negotiations, but PSPs utilize a shared agreement model. Planet Fitness includes an addendum that shifts part of the merchant responsibility to the sub-merchant franchise. While the legal implications for violating laws may impact Ohana, certain responsibilities—including aspects of the PCI compliance process—remain at the franchisor level. Therefore, the final authority is held by Planet Fitness, the franchisor, not Ohana Growth Partners, the franchisee.

13 Companies are required to follow **OSHA standards**, but they don't directly implement laws like **Public Law 91-596** (the **Occupational Safety and Health Act of 1970**). OSHA's role is to create and enforce standards to prevent workplace injuries, which have significantly reduced accidents that were once common in industries like construction and manufacturing. Prior to OSHA, voluntary standards were set by organizations such as the **American Standards Association** (now **ANSI**), which established guidelines for safety equipment like protective footwear, eyewear, and headgear.

14 In a similar way, post-1980s credit industry compliance has been shaped by landmark cases such as **FTC v. Wyndham** (2015), which set a precedent for enforcing cybersecurity measures. In this case, Wyndham Worldwide Corporation failed to implement reasonable security measures, resulting in unauthorized access to customer data. The court emphasized the importance of proper controls in protecting sensitive information, which aligns with today's **PCI DSS** standards.

15 In **PCI DSS v4.0**, **Requirement 7** emphasizes the principle of **least privilege**, which dictates that individuals and systems should have only the minimum access necessary to perform their job. This requirement breaks down into several parts:

7.1.1: Requires the implementation of access control systems that enforce least privilege.

7.1.2: Mandates limiting access to the minimum level necessary for job responsibilities, which is the core definition of least privilege.

7.1.3: Involves reviewing and adjusting access privileges to ensure they align with the least privilege principle.

7.2: Focuses on the mechanisms to enforce role-based access control systems.

16 In the context of systems like those used for processing payments (e.g., **Intune** for device configurations and **iPads** used to enter payment information), PCI DSS requires that all such systems adhere to least privilege principles. For example, payment devices and access control systems must ensure that individuals can only access the information or functions necessary for their role.

17 This approach mirrors the journey from voluntary safety standards in the past to today's strict regulatory environments, both in physical safety (OSHA) and data security (PCI DSS).

18 When a franchisee violates laws such as **Personal Information Protection**, **Consumer Credit Reporting**, **Computer Crime**, or **Securities laws** by disregarding the guidance of a PCI compliance officer, the consequences unfold in several critical stages:

19 **Violation Detection and Initial Disruption**: Once a violation is detected, operations are significantly disrupted. Key business activities, such as accepting point-of-sale (POS) payments, processing online memberships, handling sensitive member data, and managing internal communications, may be suspended. The disruption continues as a **crisis management team**—comprising legal counsel, compliance officers, and IT specialists—conducts an internal investigation. These efforts aim to assess the scope of the breach, determine the cause, and establish next steps.

20 **Stakeholder Notifications**: Based on the nature of the violation, different stakeholders must be notified. Breaches involving personal information require notifying affected individuals and relevant regulatory bodies, often in compliance with laws such as the **General Data**

Protection Regulation (GDPR) or **California Consumer Privacy Act (CCPA)**. Securities violations necessitate communication with investors and the **Securities and Exchange Commission (SEC)**. For breaches involving payment card data, notification to the **Secret Service** is mandatory, which will coordinate with other federal agencies like the **Department of Homeland Security (DHS)** and the **FBI**. These investigations focus on the point of entry for the breach and its responsible parties.

21 **Public Disclosure and Brand Impact**: The incident and subsequent investigation findings are typically made public, damaging the brand's reputation. This impact is often reflected in the company's stock price, with the breach leading to loss of consumer confidence and business relationships.

22 **Financial Penalties**: The financial consequences are severe. Violations of **personal information protection** laws can result in substantial fines from regulatory bodies like the **Federal Trade Commission (FTC)** and state attorneys general, which range from hundreds of thousands to millions of dollars. The franchisee may also face costs associated with offering **credit monitoring services** to affected individuals. For **consumer credit reporting** violations, regulatory penalties can run into millions, with additional legal settlements.

23 Breaches related to **computer crimes** can lead to millions in fines and legal fees, alongside the costs of upgrading cybersecurity measures. For **securities violations**, franchisees face significant penalties from the **SEC**, class-action lawsuits, and the costly process of correcting financial disclosures—resulting in settlements that can reach tens of millions of dollars.

24 These stages illustrate the cascading effects of non-compliance, from operational disruptions and legal investigations to hefty financial penalties and lasting reputational damage.

25 The legal landscape becomes increasingly challenging. Personal information protection breaches trigger class-action lawsuits and rigorous regulatory investigations, with legal costs reaching several million dollars. Consumer credit reporting violations lead to legal actions by consumers and enforcement measures by regulatory agencies, resulting in further legal expenses and settlements. Computer crime violations result in criminal prosecutions, civil lawsuits, and compulsory corrective measures, all contributing to substantial legal costs. Securities violations prompt SEC investigations, shareholder lawsuits, and criminal charges for fraudulent activities, leading to extensive legal battles and financial penalties.

26 Operational impacts are unavoidable. Addressing a personal information protection breach diverts resources to remediation efforts, disrupting services and necessitating enhanced security protocols. This disruption leads to lost revenue and additional costs associated with restoring normal operations. Consumer credit reporting violations compel the franchisee to overhaul compliance procedures and undergo rigorous operational audits, increasing administrative burdens and costs. In the wake of a computer crime breach, the franchisee implements stringent cybersecurity measures and upgrades their systems, incurring significant expenses. Securities violations necessitate restating financials, revising business practices, and dealing with increased scrutiny from investors and regulators, all of which require substantial effort and financial investment.

27 The brand's reputation continues to suffer, compelling the franchisor to act decisively to protect its integrity. The franchisor imposes stricter compliance requirements and increased oversight on all the franchise groups. The offending franchisee, under constant pressure, fears the franchisor will terminate their relationship, potentially bankrupting the company, and the other groups will see this as an opportunity to encourage the franchisor to address this issue by selling them or a collective of groups the ADA rights. Since the processor agreement is shared across the entire brand, a single franchisee's failure has widespread repercussions, leading to increased scrutiny, compliance measures, and damaged business relationships for all associated franchisees. The potential loss of these relationships should be a cause for immediate action.

28 The financial implications of non-compliance can be severe. Lowering the cost of acquisition to the interested parties and threatening the offending franchisee's ability to resolve their financial obligations post-sale, which could extend into the financial sources used by the groups as the brand risk is now seen differently. If another group was undergoing a significant refinancing this change could result in the terms being adjusted or offers withdrawn. This is a potentially catastrophic moment for the entire brand, which has the franchisee groups leveraging this financial lifecycle to eradicate some or all of their deferment and lowering their EBIDTA, which further hurts their refinance options. The combination of lower stock pricing, groups being devalued, and other factors will be seen in PFHQs next deal with the SEC.

29 Officers who fear criminal charges face personal fines and legal actions that can severely impact their professional reputations and future career prospects.

30 Disregarding the guidance of the organization's compliance officer and failing to adhere to PCI compliance **may constitute negligence** and breach of contract. This action undermines federal, state, and local laws related to personal information protection, consumer credit reporting, computer crime, and securities laws, which PCI compliance aims to uphold. PCI compliance sets industry standards that help ensure companies do not willfully violate regulations designed to protect the public interest. Violating these standards risks eroding public trust in credit card companies and banks, which rely on and contractually mandate PCI compliance to safeguard public safety and prevent harmful practices.

31 The Plaintiff's civil lawsuit does not address certain actions related to access requests and information withholding. There appear to be discrepancies between the events as they occurred and how they are presented in the lawsuit. A law firm involved in the case was previously accused of negligence by the Defendant. Ongoing legal issues between the parties involve matters that may not have been properly handled.

II DE FACTO LAW

OVERVIEW

32 Credit card companies, banks, processors, and other financial entities have taken proactive steps to maintain public trust by safeguarding the sensitive data they transmit, process, and store for billions of customers worldwide. When a business wants to accept payment cards, they enter into a legal relationship with a **Payment Service Provider (PSP)**, **Payment Facilitator (PayFac)**, **Payment Aggregator**, or similar entity. These entities maintain an environment that processes payments in compliance with the laws and standards required of all participants in the payment ecosystem.

33 Historically, companies that attempted to process their own payments often failed to invest adequately in security, resulting in vulnerabilities. Today, far more **oversight and certification** is required to ensure payments are processed securely. Regardless of how a business becomes a merchant in the payment card industry, its contract typically transfers collective obligations and liabilities to the business, mandating compliance with **Payment Card Industry Data Security Standards (PCI DSS)**.

34 Businesses are directly responsible for complying with **PCI DSS**, and failure to do so—especially in cases of **willful non-compliance**—can result in significant legal repercussions. PCI DSS compliance is a critical security standard, and non-adherence exposes companies to both legal and financial risks. Companies must ensure their payment processing systems and security measures fully align with the standards to avoid serious penalties and broader regulatory actions.

35 The critical flaw in the system is that compliance companies operate as independent businesses, allowing clients to switch providers freely. When this happens, companies will inevitably replace the firm that meets the requirements with one that does exactly what the company wants, even if it doesn't meet compliance standards. It’s as absurd as suspending an employee who denies an unreasonable request, offers alternatives that are ignored, provides a solution that’s accepted but never acted upon, and then, days later, is subjected to an elaborate ruse designed to torment them for hours. The next day, a lawsuit is filed against the employee, accusing them of refusing to do what they had already offered and resolved, as a pretext for denying their FMLA leave or ADA accommodation to take the day off.

36 It's just as nonsensical to think that a business looking for a certificate of compliance will choose the company that enforces stricter standards over the one that downplays requirements and falsely claims that no state or federal laws enforce PCI DSS. While it may have once been technically true that no statute explicitly mandated PCI compliance, today, not "playing ball" puts businesses at a competitive disadvantage in the PCI QSA industry. These QSA companies go on tour, speaking at industry events, where they carefully tailor their messaging to decision-makers, reassuring them with soft language that minimizes industry-specific risks. For example, when approaching a university that processes payments across large, hard-to-secure areas, QSA firms will focus on limiting who is technically required to comply with PCI DSS. They then get contracts to help the university bypass restrictions, working with vendors and other entities, even if the university staffs, profits from, and runs those operations. These firms and the business that hire them don't care if this negligence places protected data at risk just like Ohana demonstrated their lack of concern for following FMLA and ADA law that interfered with the day they had planned involving tormenting the person who is on FMLA for panic attacks.

37 Remember, Justin Drummond affirmed that he gave the order and Richard Hartman was acting as instructed and planned. That plan involved a 12-hour day of gaslighting me into believing that my coworkers, friends, family, and I were all in danger That manipulation was deemed more important than accepting the access I had offered on the 10th and 11th and prevented me from resting and making use of my FMLA leave on the 13th.

38 I also remind the court that **Daniel Levette's Affidavit** states he was able to gain access to the system and obtain a **Global Administrator role** by working with another person who had

administrative access. This is central to the Plaintiff's case. The only refusal was HEA refusing to reply to get access and Justin Drummond refusing to accept access 2 days before. I had fulfilled my duty in upholding PCI compliance and to them in finding a way to facilitate their request.

39 Daniel Levett of Hartman Executive Advisors(HEA, affirms that both Ohana and HEA always had access and they never needed an injunction or this lawsuit.

40 I say this with the highest level of respect for the court. Some of the best people I have known were judges, so I understand the workload and the difficulty in maintaining the facts of so many cases. However, these issues are not difficult to spot. The employment contract omits an entire section and is clearly missing a page or more. It's a hyperlink, and the rules are clear: hyperlinks are, by absolute definition, not part of the record, which means it's inappropriate for it to be the lead and sole technical source.

41 Then there are two affidavits in which they claim to have no access yet assert personal knowledge about how these complex systems are configured. Their roles in the Planet Fitness franchisee are the Head of HR and the President. No claim of technical expertise is made directly, and it's never provided—even when they tell the court that I am their technical expert. In that same moment, they are showing and telling the court they have no idea and are not technical.

42 Then you have HB925, which indicates that the court opinion and legislative intent of the law cited in Complaint 3 are specific and exact. There is no way that what Brennen submitted is included in that body of text, which clearly means it does not apply. Yet, a criminal statute

remains on the record for a civil case that has no jurisdiction over it. I am not splitting hairs or claiming a technicality because it's not a minor problem—the entire filing should have been rejected and handed back to them.

43 Before Robert Brennen even wrote down an invalid email address—and before he used it to create a false record claiming he had made efforts to reach me, and it was valid—from 9 p.m. to noon he had also conducted an investigation to satisfy the ex parte TRO, because that is what happened next. All those issues now also had new issues to give pause. It continues with Brennen claiming the scheduling rule is totally different, and somehow people who spend all day scheduling didn't notice that Brennen is citing a timeline that isn't like all the other schedules. I really thought the judge was going to say the obvious and reschedule because he did notice, and he said, "This is really fast." As he stood there looking at the pro se and the three or four attorneys on the side—the filing, injunctions, scheduling for show cause, and two principals and other attorneys versus the shaking, twitching pro se—no further explanation was needed.

44 It doesn't require a person to read more than the few pages related to the events they are ruling on to spot problems that require immediate remedy. In this regard, this situation either reflects a scenario where inherently Robert Brennen or the law firm itself biases the court with its mere presence to create prejudice; the assumed negative bias against all pro se litigants prejudices them to the point where the court itself needs remedy; or the fraudulent actions of Robert Brennen were extremely effective, rendering the need for a new lawsuit with judges who have not already been affected. However, Ohana never had a basis for claim, and I doubt they will be successful if they tried again.

C Judicial Enforcement Essential to Public Interest

45 Companies implement standards that provide a framework for compliance with the law. Sometimes those standards are created by the legislature, and other times the industry implements standards to avoid oversight. In the rare case of PCI DSS, the FTC is moving closer and closer to not just enforcing PCI DSS, but perhaps one day even requiring compliance with it. However, Nevada beat them to it, and PCI DSS is codified into law there, and compliance is mandatory and enforced by the government. Washington state went the other way and codified it as a shield where compliance protects, and non-compliance makes it easier to prosecute you. Below are some notable laws and then a section-by-section analysis of the PCI DSS requirements and the application of the laws that relate to Ohana Growth Partners' operations in Washington, California, Tennessee, Florida, DC, and Maryland. I provide this list not as a comprehensive list to rely on, but to demonstrate the number of laws and the number of ways that a single mistake could place the company in legal jeopardy.

> "Neither the U.S. Government nor any state or local government is involved in, is responsible for, or maintains enforcement mechanisms associated with PCI DSS. The PCI DSS is not a federal, state, or local law or regulation. Thus, there are no "federal compliance requirements" associated with the PCI DSS, as asserted by Defendant Dillon-Capps."

The Affidavit of Randall Romes, ¶10
[Provided as Ex. 9E-1]

Fact 1: Nevada (Nev. Rev. Stat. § 603A.215(1)) had codified the enforcement of PCI DSS Compliance into state law.

> "A data collector that accepts a payment card in connection with the sale of goods or services shall comply with the current version of the Payment Card Industry Data Security Standards, as adopted by the Payment Card Industry Security Standards Council or its successor organization."

Fact 2: Washington (Rev. Code Wash. § 19.255.020(2)) has codified liability protection for maintaining PCI DSS Compliance.

> "A processor, business, or vendor that is certified compliant with the Payment Card Industry Data Security Standards by an annual security assessment conducted no more than one year prior to the breach is not liable under this section."

Fact 3: In Massachusetts, **201 CMR 17.03(2)(b)** and **201 CMR 17.04(1)** enforce implementation and compliance of a cyber security standard like PCI DSS.

> **201 CMR 17.03(2)(b)** "every comprehensive information security program shall be consistent with the safeguards for protection of personal information and shall contain administrative, technical, and physical safeguards appropriate to...the size, scope, and type of business"
> **201 CMR 17.04(1)** "implementing and maintaining a comprehensive information security program."

Fact 4: Courts have acknowledged PCI DSS as a critical element of maintaining reasonable security practices. For instance, in **Re: TJX Companies Retail Security Breach Litigation, 564 F.3d 489 (1st Cir. 2009)**, the court recognized that failure to comply with PCI DSS could lead to significant legal liability under state consumer protection laws.

Fact 5: The Federal Trade Commission (FTC) has also used PCI DSS as a benchmark for reasonable security practices. In cases like **FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015)**, the FTC has cited the failure to implement PCI DSS as evidence of inadequate security measures, which can constitute an unfair practice under the FTC Act.

Fact 6: Enforcement of PCI DSS Requirements is codified in every state and the District of Columbia.

1 Requirement 1: Secured Networks

1.0 ESTABLISH AND IMPLEMENT FIREWALL AND ROUTER CONFIGURATION STANDARDS

Fact 7: Sarbanes-Oxley Act (SOX), 15 U.S.C. § 7262(b): Requires companies to establish and maintain effective internal controls, including firewall and router configuration standards, to protect financial data integrity.

Fact 8: Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030: Prohibits unauthorized access to protected computers, emphasizing the need for secure firewall and router configurations to prevent unauthorized network access.

Fact 9: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a): Mandates that businesses implement reasonable security measures, which includes establishing and maintaining firewall and router configurations to protect personal information.

Fact 10: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107: Requires businesses to implement security measures that include establishing secure network configurations to protect personal information.

Fact 11: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171: Requires businesses to take reasonable measures to secure personal information, including implementing and maintaining effective firewall and router configurations.

Fact 12: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010: Requires businesses to implement security controls that include proper network configurations to protect personal data from unauthorized access.

Fact 13: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1): Mandates the implementation of reasonable security procedures, which includes secure firewall and router configurations to protect consumer data.

Fact 14: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.): Requires businesses to implement reasonable security measures, including firewall and router configurations, to protect personal information from unauthorized access.

1.1 SEGMENT CDE NETWORKS FROM OTHER NETWORKS

Fact 15: Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030: Supports the necessity of restricting connections between untrusted networks and protected systems to prevent unauthorized access to cardholder data.

Fact 16: Federal Trade Commission Act (FTC Act), 15 U.S.C. § 45(a): Prohibits unfair practices in commerce, which includes failing to restrict network connections that could lead to unauthorized access to sensitive data.

Fact 17: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a): Requires businesses to restrict network access to protect personal information, which aligns with the need for controlled firewall and router configurations.

Fact 18: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107: Emphasizes the importance of restricting network access between untrusted networks and systems storing personal data.

Fact 19: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171: Mandates the implementation of security measures to restrict unauthorized network connections to systems containing personal information.

Fact 20: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010: Requires businesses to implement measures to restrict network access, particularly between untrusted networks and systems containing personal data.

Fact 21: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1): Requires reasonable security procedures, including restricting network access to systems containing consumer data.

Fact 22: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.): Requires businesses to restrict network connections between untrusted networks and systems containing personal information to prevent unauthorized access.

1.2 PROHIBIT DIRECT PUBLIC ACCESS TO CARDHOLDER DATA ENVIRONMENT SYSTEMS

Fact 23: Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030: Enforces the prohibition of direct public access to protected systems to prevent unauthorized access to sensitive data.

Fact 24: Sarbanes-Oxley Act (SOX), 15 U.S.C. § 7262(b): Requires companies to implement controls that prevent direct public access to financial systems, aligning with secure firewall and network configurations.

Fact 25: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a): Mandates the prevention of direct public access to systems containing personal information to protect against unauthorized access.

Fact 26: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107: Requires businesses to implement measures that prohibit direct public access to systems containing personal data.

Fact 27: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171: Requires businesses to secure systems against direct public access to protect personal information.

Fact 28: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010: Mandates that businesses prohibit direct public access to systems containing personal data to prevent unauthorized access.

Fact 29: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1): Requires reasonable security measures that include prohibiting direct public access to systems containing consumer data.

Fact 30: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.): Requires businesses to prevent direct public access to systems containing personal information to protect against unauthorized access.

1.3 IMPLEMENT FIREWALLS ON INTERNET-ENABLED PERSONAL DEVICES ACCESSING THE CDE

Fact 31: Federal Trade Commission Act (FTC Act), 15 U.S.C. § 45(a): Prohibits unfair or deceptive practices, which may include failing to implement adequate security measures like personal firewalls on devices accessing sensitive data.

Fact 32: Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030: Supports the need for personal firewalls on devices to prevent unauthorized access to protected systems when outside the corporate network.

Fact 33: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a): Requires businesses to implement security measures, such as personal firewalls, to protect personal information on devices accessing sensitive data remotely.

Fact 34: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107: Mandates the implementation of security measures like personal firewalls on devices used to access personal data outside the secure network.

Fact 35: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171: Requires businesses to implement security measures such as personal firewalls on mobile devices used to access personal information remotely.

Fact 36: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010: Mandates that businesses implement personal firewalls on devices to protect personal data accessed remotely.

Fact 37: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1): Requires the implementation of reasonable security measures, including personal firewalls on devices accessing consumer data remotely.

Fact 38: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.): Requires businesses to implement personal firewalls on devices that access personal information outside the secure network.

1.4 DOCUMENT, IMPLEMENT, AND ENFORCE FIREWALL SECURITY POLICIES AND PROCEDURES

Fact 39: Sarbanes-Oxley Act (SOX), 15 U.S.C. § 7262(b): Requires that security policies, including those related to firewall management, be documented, and communicated as part of maintaining effective internal controls.

Fact 40: Federal Trade Commission Act (FTC Act), 15 U.S.C. § 45(a): May consider the failure to document and communicate firewall management policies as an unfair practice.

Fact 41: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a): Mandates that businesses document and implement security policies, including those for firewall management, to protect personal information.

Fact 42: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107: Requires businesses to document and communicate security policies, including firewall management procedures, to protect personal information.

Fact 43: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171: Requires businesses to ensure that security policies, including those for managing firewalls, are documented, in use, and known to relevant personnel.

Fact 44: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010: Mandates that businesses document and implement security policies for firewall management to protect personal data.

Fact 45: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1): Requires that businesses document and enforce security policies, including those related to firewall management, to protect consumer data.

Fact 46: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.): Requires businesses to ensure that security policies, including those for managing firewalls, are documented and effectively communicated.

2 Requirement 2: Secured Systems

2.0 Change Vendor Defaults

Fact 47: Federal Trade Commission Act (FTC Act), 15 U.S.C. § 45(a) prohibits unfair or deceptive practices, which include using vendor-supplied defaults for system passwords and other security parameters, exposing consumers to potential risks.

Fact 48: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801-6809 mandates financial institutions to protect the confidentiality of customer information, which includes ensuring that vendor-supplied defaults are not used for system passwords and security parameters.

Fact 49: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.308(a)(5)(ii)(B) requires security awareness training, including protection from using vendor-supplied defaults for security settings, which aligns with the requirement to change default passwords and settings.

Fact 50: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a) requires businesses to implement reasonable security measures, including changing vendor-supplied defaults for system passwords and other security parameters to protect personal information.

Fact 51: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107 mandates that businesses change vendor-supplied defaults for system passwords and other security parameters to protect personal information from unauthorized access.

Fact 52: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171(2) requires businesses to take reasonable measures, including changing vendor-supplied defaults for system passwords and other security parameters, to protect personal information.

Fact 53: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010 mandates that businesses implement security measures, including changing vendor-supplied defaults for system passwords and security parameters to protect personal data.

Fact 54: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1) requires businesses to implement reasonable security procedures, including changing vendor-supplied defaults for system passwords and other security parameters to protect consumer data.

Fact 55: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.) mandates that businesses protect personal information by ensuring that vendor-supplied defaults for system passwords and other security parameters are changed.

2.1 ALWAYS CHANGE VENDOR-SUPPLIED DEFAULTS BEFORE INSTALLING A SYSTEM ON THE NETWORK

Fact 56: Federal Trade Commission Act (FTC Act), 15 U.S.C. § 45(a) prohibits unfair or deceptive practices, including failing to change vendor-supplied defaults before installing a system on the network, which could lead to unauthorized access to sensitive data.

Fact 57: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801-6809 mandates financial institutions to change vendor-supplied defaults before installing systems on the network to protect the confidentiality and security of customer information.

Fact 58: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.308(a)(5)(ii)(B) requires organizations to provide training that includes changing vendor-supplied defaults before installing systems on the network to protect sensitive data.

Fact 59: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a) mandates that businesses change vendor-supplied defaults before installing a system on the network to protect personal information.

Fact 60: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107 requires businesses to change vendor-supplied defaults before installing systems on the network to prevent unauthorized access to personal information.

Fact 61: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171(2) mandates that businesses change vendor-supplied defaults before installing systems on the network to protect personal information.

Fact 62: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010 requires businesses to change vendor-supplied defaults before installing systems on the network to protect personal data from unauthorized access.

Fact 63: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1) mandates that businesses change vendor-supplied defaults before installing systems on the network to protect consumer data.

Fact 64: The **District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.)** requires businesses to change vendor-supplied defaults before installing systems on the network to protect personal information.

2.2 DEVELOP CONFIGURATION STANDARDS FOR ALL SYSTEM COMPONENTS. ASSURE THAT THESE STANDARDS ADDRESS ALL KNOWN SECURITY VULNERABILITIES AND ARE CONSISTENT WITH INDUSTRY-ACCEPTED SYSTEM HARDENING STANDARDS

Fact 65: Sarbanes-Oxley Act (SOX), 15 U.S.C. § 7262(b), requires companies to establish and maintain internal controls, which include developing configuration standards for system components that address security vulnerabilities.

Fact 66: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801-6809 mandates that financial institutions develop configuration standards for system components that address known security vulnerabilities to protect customer information.

Fact 67: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.308(a)(1)(ii)(B) requires the implementation of security management processes, which include developing configuration standards for system components to protect sensitive data.

Fact 68: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a) requires businesses to develop configuration standards for system components to address security vulnerabilities and protect personal information.

Fact 69: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107 mandates that businesses develop configuration standards for system components that address security vulnerabilities to protect personal information.

Fact 70: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171 requires businesses to develop configuration standards for system components to address security vulnerabilities and protect personal information.

Fact 71: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010 mandates that businesses develop configuration standards for system components to address known security vulnerabilities and protect personal data.

Fact 72: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1) requires businesses to develop configuration standards for system components to address security vulnerabilities and protect consumer data.

Fact 73: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.) mandates that businesses develop configuration standards for system components that address security vulnerabilities to protect personal information.

Fact 74: 2.3 Encrypt all non-console administrative access using strong cryptography Federal Information Security Management Act (FISMA), 44 U.S.C. § 3544 requires federal agencies to encrypt non-console administrative access using strong cryptography to protect sensitive data.

Fact 75: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801-6809 mandates that financial institutions encrypt non-console administrative access using strong cryptography to protect the confidentiality and security of customer information.

Fact 76: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.312(a)(2)(iv) requires the implementation of encryption for non-console administrative access to protect sensitive health information.

Fact 77: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(b) mandates that businesses encrypt non-console administrative access using strong cryptography to protect personal information.

Fact 78: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107 requires businesses to encrypt non-console administrative access using strong cryptography to prevent unauthorized access to personal information.

Fact 79: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171 mandates that businesses encrypt non-console administrative access using strong cryptography to protect personal information.

Fact 80: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010 requires businesses to encrypt non-console administrative access using strong cryptography to protect personal data.

Fact 81: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1) requires businesses to implement encryption for non-console administrative access to protect consumer data.

Fact 82: The **District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.)** mandates that businesses encrypt non-console administrative access using strong cryptography to protect personal information.

2.3 REQUIREMENT 2.4 HAS NO FEDERAL, MARYLAND, TENNESSEE, FLORIDA, WASHINGTON, CALIFORNIA, AND DC STATUTES.

2.4 ENSURE THAT SECURITY POLICIES AND OPERATIONAL PROCEDURES FOR MANAGING VENDOR DEFAULTS AND OTHER SECURITY PARAMETERS ARE DOCUMENTED, IN USE, AND KNOWN TO ALL AFFECTED PARTIES

Fact 83: Sarbanes-Oxley Act (SOX), 15 U.S.C. § 7262(b) requires companies to document and enforce internal controls, which include security policies and procedures for managing vendor defaults and other security parameters.

Fact 84: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801-6809 mandates that financial institutions document and implement security policies and procedures for managing vendor defaults and other security parameters to protect customer information.

Fact 85: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.316(a) requires the documentation and implementation of security policies and procedures for managing vendor defaults and other security parameters to protect sensitive data.

Fact 86: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a) mandates that businesses document and enforce security policies and procedures for managing vendor defaults and other security parameters to protect personal information.

Fact 87: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107 requires businesses to document and implement security policies and procedures for managing vendor defaults and other security parameters to protect personal information.

Fact 88: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171 mandates that businesses document and enforce security policies and procedures for managing vendor defaults and other security parameters to protect personal information.

Fact 89: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010 requires businesses to document and implement security policies and procedures for managing vendor defaults and other security parameters to protect personal data.

Fact 90: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1) requires businesses to document and implement security policies and procedures for managing vendor defaults and other security parameters to protect consumer data.

Fact 91: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.) mandates that businesses document and enforce security policies and procedures for managing vendor defaults and other security parameters to protect personal information.

3 Requirement 3: Secured Data

3.0 PROTECT STORED CARDHOLDER DATA

Fact 92: Federal Trade Commission Act (FTC Act), 15 U.S.C. § 45(a) prohibits unfair or deceptive practices, which includes failing to protect stored cardholder data, potentially exposing it to unauthorized access.

Fact 93: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801-6809 requires financial institutions to protect the confidentiality and security of customer information, which includes ensuring that stored cardholder data is properly secured.

Fact 94: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.312(a)(2)(iv) mandates the implementation of access controls, such as encryption, to protect stored sensitive data, which aligns with the protection of stored cardholder data.

Fact 95: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a) requires businesses to implement reasonable security measures, including protecting stored cardholder data from unauthorized access.

Fact 96: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107 mandates that businesses protect stored personal information, including cardholder data, by implementing appropriate security measures.

Fact 97: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171(2) requires businesses to take reasonable measures to protect stored personal information, including cardholder data, from unauthorized access.

Fact 98: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010 mandates that businesses implement security measures to protect stored personal data, including cardholder information, from unauthorized access.

Fact 99: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1) requires businesses to implement reasonable security procedures to protect stored consumer data, including cardholder information, from unauthorized access.

Fact 100: The **District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.)** mandates that businesses protect stored personal information, including cardholder data, from unauthorized access.

3.1 ONLY STORE REQUIRED LEGAL, REGULATORY, AND BUSINESS DATA

Fact 101: Sarbanes-Oxley Act (SOX), 15 U.S.C. § 7262(b): Requires companies to maintain effective internal controls, which includes limiting the storage of sensitive data such as cardholder information and retaining such data only as long as necessary for compliance and business needs.

Fact 102: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.310(d)(2)(i): Although primarily for health data, this regulation underscores the importance of data retention policies, including limiting storage to the minimum necessary, which can be analogous to storing cardholder data only as needed.

Fact 103: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a): Requires businesses to limit the storage of personal information, including cardholder data, and retain it only for as long as necessary to meet legal and business requirements.

Fact 104: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107: Mandates the implementation of security measures that include limiting the storage of personal information such as cardholder data and retaining it only as necessary.

Fact 105: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171(2): Requires businesses to protect personal information, including limiting its storage and ensuring it is retained only for the period necessary to fulfill legal and business obligations.

Fact 106: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010: Mandates that businesses limit the storage of personal data, including cardholder

data, to what is necessary for legal and business purposes, thereby minimizing the risk of unauthorized access.

Fact 107: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1): Requires the implementation of reasonable security procedures, which include limiting the storage of personal data such as cardholder information and retaining it only as necessary.

Fact 108: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.): Mandates that businesses limit the storage of personal information, including cardholder data, to what is necessary for legal and business purposes.

3.2 Never Store Sensitive Authentication Data

Fact 109: Federal Trade Commission Act (FTC Act), 15 U.S.C. § 45(a): Prohibits unfair or deceptive practices in commerce, which could include the retention of sensitive authentication data after authorization, as it exposes consumers to unnecessary risk.

Fact 110: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801-6809: Mandates financial institutions to protect the confidentiality of customer information, which includes ensuring that sensitive authentication data is not stored post-authorization.

Fact 111: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a): Requires businesses to implement security measures that include prohibiting the storage of sensitive authentication data after authorization.

Fact 112: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107: Mandates the implementation of security measures that prohibit the retention of sensitive authentication data post-authorization.

Fact 113: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171: Prohibits the storage of sensitive authentication data after authorization to protect personal information.

Fact 114: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010: Requires businesses to implement security controls that prohibit the storage of sensitive authentication data after it is no longer necessary for business purposes.

Fact 115: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1): Requires the implementation of reasonable security procedures, including prohibiting the storage of sensitive authentication data after authorization.

Fact 116: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.): Mandates that businesses do not retain sensitive authentication data after authorization to ensure the protection of personal information.

3.3 Limit Displayed PAN to First Six and Last Four

Fact 117: Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681c(g): Requires that credit card numbers be truncated on receipts, aligning with the PCI DSS requirement to mask the Primary Account Number (PAN) when displayed.

Fact 118: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3504(b): Requires businesses to mask the PAN when displaying credit card numbers to protect personal information.

Fact 119: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107: Mandates that businesses mask PANs when displayed, ensuring that only the first six and last four digits are visible.

Fact 120: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171: Requires businesses to ensure that when PANs are displayed, they are truncated so that only the first six and last four digits are visible.

Fact 121: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010: Mandates that businesses mask PANs when displayed, allowing only the first six and last four digits to be visible to protect personal data.

Fact 122: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1): Requires businesses to mask PANs when displayed, ensuring that only the first six and last four digits are shown to protect consumer data.

Fact 123: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.): Requires businesses to mask PANs when displaying cardholder information, limiting the visible digits to the first six and last four.

3.4 Obfuscate Stored PAN Using Strong Cryptography

Fact 124: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801-6809: Requires financial institutions to protect the confidentiality and integrity of customer information, which includes rendering PAN unreadable through encryption or other strong cryptographic methods.

Fact 125: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.312(a)(2)(iv): Although primarily for health information, HIPAA's requirements for encryption align with the necessity to render PAN unreadable wherever it is stored.

Fact 126: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(b): Mandates the use of strong encryption or other methods to render PAN unreadable wherever it is stored, to protect personal information.

Fact 127: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107: Requires businesses to render PAN unreadable by using strong cryptography wherever it is stored.

Fact 128: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171: Mandates that businesses render PAN unreadable wherever it is stored, including on digital and backup media, by using strong cryptography.

Fact 129: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010: Requires businesses to protect stored personal data by rendering PAN unreadable through encryption or other cryptographic methods.

Fact 130: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1): Requires businesses to use strong cryptography to render PAN unreadable wherever it is stored, protecting consumer data.

Fact 131: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.): Mandates the use of strong cryptographic methods to render PAN unreadable wherever it is stored, protecting personal information.

3.5 DOCUMENT AND IMPLEMENT PROCEDURES TO SECURE CRYPTOGRAPHIC KEYS

Fact 132: Sarbanes-Oxley Act (SOX), 15 U.S.C. § 7262(b): Requires the documentation and implementation of internal controls, which includes securing cryptographic keys to protect stored cardholder data.

Fact 133: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801-6809: Mandates that financial institutions implement controls to protect encryption keys used to secure customer information.

Fact 134: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(b): Requires businesses to document and implement procedures to protect cryptographic keys used to secure stored personal data.

Fact 135: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107: Mandates the implementation of procedures to protect encryption keys used to secure stored personal information from disclosure and misuse.

Fact 136: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171: Requires businesses to implement procedures to protect cryptographic keys used to secure stored personal data against unauthorized disclosure and misuse.

Fact 137: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010: Mandates that businesses implement and document procedures to secure encryption keys used to protect stored personal data.

Fact 138: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1): Requires businesses to document and implement procedures to protect cryptographic keys used to secure stored consumer data.

Fact 139: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.): Mandates that businesses implement and document procedures to protect cryptographic keys used to secure stored personal information.

Fact 140: 3.6: Fully document and implement all key management processes and procedures for cryptographic keys used for encryption of cardholder data.

Fact 141: Sarbanes-Oxley Act (SOX), 15 U.S.C. § 7262(b): Requires the full documentation and implementation of key management processes as part of internal controls to ensure the security of encrypted cardholder data.

Fact 142: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801-6809: Mandates that financial institutions fully document and implement key management processes to protect the encryption of customer information.

Fact 143: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(b): Requires businesses to fully document and implement key management processes to ensure the security of encrypted personal data.

Fact 144: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107: Mandates the full documentation and implementation of key management processes to secure encrypted personal information.

Fact 145: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171: Requires businesses to document and implement key management processes to ensure the protection of encrypted personal data.

Fact 146: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010: Mandates that businesses fully document and implement key management processes to secure encrypted personal data.

Fact 147: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1): Requires businesses to document and implement key management processes to secure encrypted consumer data.

Fact 148: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.): Mandates the full documentation and implementation of key management processes to secure encrypted personal information.

4 Requirement 4: Secured Transmission

4.0 PROTECT CARDHOLDER DATA WITH STRONG CRYPTOGRAPHY DURING TRANSMISSION OVER OPEN, PUBLIC NETWORKS

Fact 149: Federal Trade Commission Act (FTC Act), 15 U.S.C. § 45(a) prohibits unfair or deceptive practices, which includes failing to use strong cryptography to protect cardholder data during transmission over open, public networks.

Fact 150: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801-6809 mandates that financial institutions protect the confidentiality and security of customer information, which includes using strong cryptography during data transmission over public networks.

Fact 151: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.312(e)(1) requires the implementation of technical security measures, including encryption, to guard against unauthorized access to electronic protected health information during transmission, which aligns with the need to secure cardholder data during transmission.

Fact 152: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a) requires businesses to implement reasonable security measures, including the use of strong cryptography to protect personal information during transmission over open, public networks.

Fact 153: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107 mandates that businesses secure the transmission of personal information over public networks by using strong cryptography.

Fact 154: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171(2) requires businesses to take reasonable measures to protect personal information, including using strong cryptography during transmission over open networks.

Fact 155: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010 mandates that businesses implement security measures, such as strong cryptography, to protect personal data during transmission over public networks.

Fact 156: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1) requires businesses to implement reasonable security procedures, including the use of strong cryptography to protect consumer data during transmission.

Fact 157: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.) mandates that businesses protect personal information during transmission over public networks by using strong cryptography.

4.1 ENSURE STRONG CRYPTOGRAPHY AND SECURITY PROTOCOLS ARE USED TO SAFEGUARD SENSITIVE CARDHOLDER DATA DURING TRANSMISSION OVER OPEN, PUBLIC NETWORKS

Fact 158: Federal Trade Commission Act (FTC Act), 15 U.S.C. § 45(a) prohibits unfair or deceptive practices, including failing to ensure strong cryptography and security protocols are used to safeguard cardholder data during transmission over open, public networks.

Fact 159: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801-6809 mandates financial institutions to protect the confidentiality of customer information, which includes ensuring the use of strong cryptography and security protocols during transmission.

Fact 160: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.312(e)(1) requires the implementation of security measures, including encryption, to protect sensitive data during transmission, aligning with the need to safeguard cardholder data.

Fact 161: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a) requires businesses to implement reasonable security measures, including the use of strong cryptography and security protocols to protect personal information during transmission over open networks.

Fact 162: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107 mandates that businesses ensure strong cryptography and security protocols are used to protect personal information during transmission over public networks.

Fact 163: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171(2) requires businesses to implement security measures, including strong cryptography and security protocols, to protect personal information during transmission over open networks.

Fact 164: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010 mandates that businesses implement strong cryptography and security protocols to protect personal data during transmission over public networks.

Fact 165: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1) requires businesses to use strong cryptography and security protocols to safeguard consumer data during transmission over open, public networks.

Fact 166: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.) mandates that businesses ensure strong cryptography and security protocols are used to protect personal information during transmission over public networks.

4.2 NEVER SEND UNPROTECTED PANS BY END-USER MESSAGING TECHNOLOGIES (FOR EXAMPLE, E-MAIL, INSTANT MESSAGING, SMS, CHAT, ETC.)

Fact 167: Federal Trade Commission Act (FTC Act), 15 U.S.C. § 45(a) prohibits unfair or deceptive practices, including sending unprotected PANs (Primary Account Numbers) by end-user messaging technologies, which could expose sensitive data to unauthorized access.

Fact 168: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801-6809 requires financial institutions to protect customer information from unauthorized access, including prohibiting the transmission of unprotected PANs via end-user messaging technologies.

Fact 169: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.312(e)(1) mandates security measures, including encryption, to protect sensitive data during transmission, which parallels the requirement to avoid sending unprotected PANs via messaging technologies.

Fact 170: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a) requires businesses to implement security measures that prohibit the transmission of unprotected PANs via end-user messaging technologies.

Fact 171: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107 mandates that businesses prevent the transmission of unprotected PANs through end-user messaging technologies to protect personal information from unauthorized access.

Fact 172: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171(2) requires businesses to protect personal information by ensuring that PANs are not transmitted unprotected through end-user messaging technologies.

Fact 173: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010 mandates that businesses avoid sending unprotected PANs via end-user messaging technologies to protect personal data from unauthorized access.

Fact 174: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1) requires businesses to implement security measures that prevent the transmission of unprotected PANs via end-user messaging technologies.

Fact 175: The **District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.)** mandates that businesses prohibit the transmission of unprotected PANs through end-user messaging technologies to safeguard personal information.

4.3 ENSURE THE SECURITY OF PANS STORED IN FILES OR DATABASES THAT ARE RECEIVED FROM OR SENT TO THIRD PARTIES VIA END-USER MESSAGING TECHNOLOGIES

Fact 176: Federal Trade Commission Act (FTC Act), 15 U.S.C. § 45(a) prohibits unfair practices, which include failing to secure PANs stored in files or databases that are transmitted via end-user messaging technologies, exposing sensitive data to risk.

Fact 177: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801-6809 mandates that financial institutions protect stored customer information, including ensuring the security of PANs stored in files or databases transmitted to third parties via end-user messaging technologies.

Fact 178: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.312(c)(1) requires the implementation of access control measures, which align with ensuring the security of sensitive data, such as PANs, stored in files or databases transmitted via messaging technologies.

Fact 179: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a) requires businesses to secure PANs stored in files or databases transmitted via end-user messaging technologies to protect personal information.

Fact 180: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107 mandates that businesses ensure the security of PANs stored in files or databases sent to or received from third parties via end-user messaging technologies.

Fact 181: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171(2) requires businesses to protect PANs stored in files or databases during transmission to or from third parties using end-user messaging technologies.

Fact 182: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010 mandates that businesses ensure the security of PANs stored in files or databases when transmitted via end-user messaging technologies.

Fact 183: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1) requires businesses to implement security measures to protect PANs stored in files or databases that are transmitted via end-user messaging technologies.

Fact 184: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.) mandates that businesses ensure the security of PANs stored in files or databases transmitted to or from third parties via end-user messaging technologies.

5 Requirement 5: Endpoint Security

5.0 Implement and maintain policies and procedures to protect systems and networks from malicious software

Fact 185: Federal Trade Commission Act (FTC Act), 15 U.S.C. § 45(a) prohibits unfair or deceptive practices, which include failing to implement and maintain policies and

procedures to protect systems and networks from malicious software, thereby risking consumer data.

Fact 186: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801-6809 mandates financial institutions to implement policies and procedures that protect the confidentiality and security of customer information, which includes defending systems and networks against malicious software.

Fact 187: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.308(a)(5)(ii)(B) requires the implementation of procedures for guarding against, detecting, and reporting malicious software, aligning with the need to protect systems and networks.

Fact 188: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a) requires businesses to implement reasonable security measures, including policies and procedures to protect systems and networks from malicious software.

Fact 189: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107 mandates that businesses implement policies and procedures to protect systems and networks from malicious software to prevent unauthorized access to personal information.

Fact 190: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171(2) requires businesses to implement security measures, including policies and procedures to protect systems and networks from malicious software.

Fact 191: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010 mandates that businesses implement policies and procedures to protect systems and networks from malicious software to safeguard personal data.

Fact 192: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1) requires businesses to implement reasonable security procedures, including policies and procedures to protect systems and networks from malicious software to protect consumer data.

Fact 193: The **District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.)** mandates that businesses implement and maintain policies and procedures to protect systems and networks from malicious software to secure personal information.

5.1 ENDPOINT SECURITY PREVENTS MALICIOUS SOFTWARE

Fact 194: Federal Trade Commission Act (FTC Act), 15 U.S.C. § 45(a) prohibits unfair or deceptive practices in commerce, including the failure to deploy anti-malware software on systems, which could lead to unauthorized access to sensitive data.

Fact 195: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801-6809 mandates financial institutions to implement measures to protect the confidentiality and security of customer information, which includes deploying anti-malware software to safeguard systems from malicious software.

Fact 196: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.308(a)(5)(ii)(B) requires the implementation of procedures for guarding against,

detecting, and reporting malicious software, which aligns with deploying anti-malware software on affected systems.

Fact 197: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a) requires businesses to implement reasonable security measures, including the deployment of anti-malware software to protect personal information from unauthorized access via malicious software.

Fact 198: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107 mandates that businesses deploy anti-malware software on systems to prevent unauthorized access to personal information due to malicious software.

Fact 199: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171(2) requires businesses to protect personal information by deploying anti-malware software on systems commonly affected by malicious software.

Fact 200: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010 mandates that businesses implement security measures, such as deploying anti-malware software, to protect personal data from malicious software.

Fact 201: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1) requires businesses to implement reasonable security procedures, including the deployment of anti-malware software, to protect consumer data from unauthorized access due to malicious software.

Fact 202: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.) mandates that businesses deploy anti-malware software on systems to protect personal information from malicious software attacks.

5.2 ENDPOINT SECURITY MAINTAINED, UPDATED, AND LOGGED

Fact 203: Federal Trade Commission Act (FTC Act), 15 U.S.C. § 45(a) prohibits unfair practices, including failing to maintain and update anti-malware mechanisms, which could lead to inadequate protection of sensitive data and unauthorized access.

Fact 204: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801-6809 requires financial institutions to maintain up-to-date security measures, including anti-malware mechanisms, to protect the confidentiality and integrity of customer information.

Fact 205: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.308(a)(5)(ii)(B) mandates the maintenance and regular updating of anti-malware mechanisms to ensure ongoing protection against malicious software.

Fact 206: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a) requires businesses to maintain and regularly update anti-malware mechanisms to protect personal information and ensure that audit logs are generated.

Fact 207: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107 mandates the regular maintenance and updating of anti-malware mechanisms to protect personal information from unauthorized access due to outdated or ineffective security measures.

Fact 208: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171(2) requires businesses to maintain up-to-date anti-malware mechanisms that are capable of generating audit logs to protect personal information.

Fact 209: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010 mandates that businesses maintain and update anti-malware mechanisms to ensure the protection of personal data and the generation of audit logs.

Fact 210: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1) requires businesses to maintain and regularly update anti-malware mechanisms to protect consumer data from unauthorized access and ensure that audit logs are generated.

Fact 211: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.) mandates the maintenance and updating of anti-malware mechanisms to protect personal information and ensure audit logs are generated to monitor security.

5.3 ENDPOINT SECURITY PREVENTS ALTERING

Fact 212: Federal Trade Commission Act (FTC Act), 15 U.S.C. § 45(a) prohibits unfair or deceptive practices, which include allowing anti-malware mechanisms to be disabled or altered by users, leading to potential unauthorized access to sensitive data.

Fact 213: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801-6809 mandates that financial institutions ensure the active operation of anti-malware mechanisms that cannot be disabled or altered by users, except under specific management authorization, to protect customer information.

Fact 214: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.312(c)(1) requires the implementation of security measures that prevent unauthorized users from disabling or altering security mechanisms, including anti-malware protections.

Fact 215: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a) mandates that businesses ensure anti-malware mechanisms are actively running and cannot be disabled or altered by users, except with specific management authorization.

Fact 216: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107 requires businesses to ensure that anti-malware mechanisms are continuously active and cannot be disabled or altered by users, except under strict management control.

Fact 217: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171 mandates that businesses ensure anti-malware mechanisms are always active and protected from unauthorized disabling or alteration by users.

Fact 218: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010 requires businesses to ensure that anti-malware mechanisms remain active and cannot be altered or disabled by users without proper management authorization.

Fact 219: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1) requires businesses to implement security measures that ensure anti-malware mechanisms are always active and protected from unauthorized user alterations.

Fact 220: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.) mandates that businesses ensure anti-malware mechanisms remain active and cannot be disabled or altered by users without specific management authorization.

6 Requirement 6: Change Control Management

6.0 Develop and Maintain Secure Systems and Software

Fact 221: Sarbanes-Oxley Act (SOX), 15 U.S.C. § 7262(b) requires companies to establish and maintain effective internal controls, which include developing and maintaining secure systems and software to ensure the integrity of financial data.

Fact 222: Federal Trade Commission Act (FTC Act), 15 U.S.C. § 45(a) prohibits unfair or deceptive practices, including the failure to develop and maintain secure systems and software, which could lead to unauthorized access to consumer data.

Fact 223: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801-6809 mandates that financial institutions develop and maintain secure systems and software to protect the confidentiality and security of customer information.

Fact 224: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.308(a)(1)(ii)(A) requires the implementation of policies and procedures to prevent, detect, contain, and correct security violations, which includes maintaining secure systems and software.

Fact 225: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a) mandates that businesses develop and maintain secure systems and software to protect personal information from unauthorized access.

Fact 226: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107 requires businesses to develop and maintain secure systems and software to protect personal information from unauthorized access.

Fact 227: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171(2) mandates that businesses implement security measures, including the development and maintenance of secure systems and software, to protect personal information.

Fact 228: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010 mandates that businesses develop and maintain secure systems and software to protect personal data from unauthorized access.

Fact 229: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1) requires businesses to implement reasonable security procedures, including developing and maintaining secure systems and software to protect consumer data.

Fact 230: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.) mandates that businesses develop and maintain secure systems and software to protect personal information from unauthorized access.

6.1 ESTABLISH A PROCESS TO IDENTIFY SECURITY VULNERABILITIES IN A TIMELY MANNER AND ENSURE THAT ALL SYSTEM COMPONENTS AND SOFTWARE ARE PROTECTED FROM KNOWN VULNERABILITIES BY INSTALLING APPLICABLE VENDOR-SUPPLIED SECURITY PATCHES. INSTALL CRITICAL SECURITY PATCHES WITHIN ONE MONTH OF RELEASE.

Fact 231: Sarbanes-Oxley Act (SOX), 15 U.S.C. § 7262(b) requires companies to establish processes for identifying and mitigating security vulnerabilities, including timely installation of security patches, as part of maintaining effective internal controls.

Fact 232: Federal Trade Commission Act (FTC Act), 15 U.S.C. § 45(a) prohibits unfair or deceptive practices, including failing to address known security vulnerabilities in systems and software by not applying timely security patches.

Fact 233: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801-6809 mandates that financial institutions protect customer information by identifying and addressing security vulnerabilities in a timely manner, including installing critical security patches.

Fact 234: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.308(a)(8) requires regular evaluations to ensure that security measures are adequate, which includes applying security patches to protect against known vulnerabilities.

Fact 235: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a) requires businesses to identify security vulnerabilities and apply vendor-supplied security patches promptly to protect personal information.

Fact 236: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107 mandates the timely installation of security patches to address known vulnerabilities and protect personal information.

Fact 237: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171 mandates that businesses implement processes to identify and mitigate security vulnerabilities, including the installation of security patches within a specified time frame.

Fact 238: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010 requires businesses to protect personal data by identifying and addressing security vulnerabilities through the installation of critical security patches.

Fact 239: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1) requires businesses to implement security measures to address known vulnerabilities and ensure timely installation of critical security patches.

Fact 240: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.) mandates that businesses identify and address security vulnerabilities in a timely manner by installing critical security patches to protect personal information.

6.2 DEVELOP INTERNAL AND EXTERNAL SOFTWARE APPLICATIONS SECURELY, WITH PROPER TESTING AND APPROVAL PROCESSES. ENSURE THAT APPLICATIONS ARE DEVELOPED IN ACCORDANCE WITH INDUSTRY BEST PRACTICES AND ARE REVIEWED FOR VULNERABILITIES BEFORE BEING DEPLOYED.

Fact 241: Sarbanes-Oxley Act (SOX), 15 U.S.C. § 7262(b) requires companies to implement controls that ensure the secure development of internal and external software applications, including proper testing and approval processes, to maintain data integrity.

Fact 242: Federal Trade Commission Act (FTC Act), 15 U.S.C. § 45(a) prohibits unfair practices, which include deploying software applications that have not been securely developed or tested for vulnerabilities, thereby risking consumer data.

Fact 243: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801-6809 mandates that financial institutions develop and deploy software applications securely, ensuring they are tested for vulnerabilities and comply with industry best practices to protect customer information.

Fact 244: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.308(a)(5)(ii)(A) requires organizations to implement security awareness and training programs for employees, which includes ensuring secure software development practices.

Fact 245: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a) mandates that businesses develop and deploy software applications securely, ensuring proper testing for vulnerabilities and adherence to industry standards to protect personal information.

Fact 246: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107 requires businesses to develop internal and external software applications securely, with proper testing and review processes, to protect personal information.

Fact 247: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171 requires businesses to ensure that software applications are developed securely, tested for vulnerabilities, and comply with industry best practices to protect personal information.

Fact 248: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010 mandates that businesses develop and deploy software applications securely, ensuring they are tested for vulnerabilities and adhere to industry standards to protect personal data.

Fact 249: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1) requires businesses to ensure that software applications are securely developed, tested for vulnerabilities, and comply with industry best practices to protect consumer data.

Fact 250: The **District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.)** mandates that businesses develop internal and external software applications securely, with proper testing and approval processes, to protect personal information.

6.3 ENSURE THAT CHANGE CONTROL PROCESSES ARE FOLLOWED FOR ALL SYSTEM AND SOFTWARE CONFIGURATION CHANGES, WITH TESTING, DOCUMENTATION, AND BACK-OUT PROCEDURES IN PLACE.

Fact 251: Sarbanes-Oxley Act (SOX), 15 U.S.C. § 7262(b) requires companies to implement change control processes that ensure all system and software configuration changes are properly tested, documented, and have back-out procedures to maintain data integrity.

Fact 252: Federal Trade Commission Act (FTC Act), 15 U.S.C. § 45(a) prohibits unfair practices, including failing to follow change control processes for system and software changes, which could lead to unauthorized access or data loss.

Fact 253: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801-6809 mandates that financial institutions implement change control processes for system and software changes, ensuring they are tested, documented, and reversible to protect customer information.

Fact 254: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.308(a)(8) requires regular evaluations and updates to security measures, which includes implementing change control processes for all system and software changes to protect sensitive data.

Fact 255: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a) mandates that businesses implement change control processes for all system and software configuration changes, including proper testing, documentation, and back-out procedures to protect personal information.

Fact 256: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107 requires businesses to implement change control processes for all system and software configuration changes, ensuring proper testing, documentation, and back-out procedures to protect personal information.

Fact 257: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171 mandates that businesses implement change control processes for all system and software configuration changes, including proper testing, documentation, and back-out procedures to protect personal information.

Fact 258: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010 requires businesses to follow change control processes for all system and software configuration changes, ensuring proper testing, documentation, and back-out procedures to protect personal data.

Fact 259: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1) requires businesses to implement change control processes for all system and software configuration changes, ensuring proper testing, documentation, and back-out procedures to protect consumer data.

Fact 260: The **District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.)** mandates that businesses follow change control processes for all system and software configuration changes, including proper testing, documentation, and back-out procedures to protect personal information.

6.4 FOLLOW SECURE CODING GUIDELINES AND ENSURE THAT SECURE CODING TECHNIQUES ARE APPLIED. TRAIN DEVELOPERS IN SECURE CODING TECHNIQUES, INCLUDING HOW TO AVOID COMMON CODING VULNERABILITIES.

Fact 261: Sarbanes-Oxley Act (SOX), 15 U.S.C. § 7262(b) requires companies to ensure that software development follows secure coding guidelines and that developers are trained in secure coding techniques to maintain the integrity of financial data.

Fact 262: Federal Trade Commission Act (FTC Act), 15 U.S.C. § 45(a) prohibits unfair practices, which include failing to follow secure coding guidelines or to train developers in secure coding techniques, potentially leading to vulnerabilities in software.

Fact 263: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801-6809 mandates that financial institutions follow secure coding guidelines and train developers in secure coding techniques to protect customer information from software vulnerabilities.

Fact 264: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.308(a)(5)(ii)(A) requires the implementation of security awareness and training programs, including secure coding practices, to protect sensitive health information.

Fact 265: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a) mandates that businesses follow secure coding guidelines and train developers in secure coding techniques to protect personal information.

Fact 266: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107 requires businesses to follow secure coding guidelines and ensure that developers are trained in secure coding techniques to protect personal information.

Fact 267: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171 mandates that businesses follow secure coding guidelines and train developers in secure coding techniques to protect personal information from vulnerabilities in software.

Fact 268: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010 requires businesses to follow secure coding guidelines and ensure that developers are trained in secure coding techniques to protect personal data.

Fact 269: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1) requires businesses to follow secure coding guidelines and train developers in secure coding techniques to protect consumer data.

Fact 270: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.) mandates that businesses follow secure coding guidelines and train developers in secure coding techniques to protect personal information.

6.5 REQUIREMENT 6.5 HAS NO FEDERAL, MARYLAND, TENNESSEE, FLORIDA, WASHINGTON, CALIFORNIA, AND DC STATUTES AT THIS TIME.

6.6 ENSURE THAT ALL PUBLIC-FACING WEB APPLICATIONS ARE PROTECTED AGAINST KNOWN ATTACKS BY PERFORMING APPLICATION VULNERABILITY ASSESSMENTS OR BY IMPLEMENTING AN AUTOMATED TECHNICAL SOLUTION THAT DETECTS AND PREVENTS WEB-BASED ATTACKS.

Fact 271: Federal Trade Commission Act (FTC Act), 15 U.S.C. § 45(a) prohibits unfair or deceptive practices, which include failing to protect public-facing web applications against known attacks, potentially exposing consumers to harm.

Fact 272: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801-6809 mandates that financial institutions protect public-facing web applications by conducting vulnerability assessments or implementing automated solutions to prevent web-based attacks.

Fact 273: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.308(a)(1)(ii)(A) requires the implementation of security measures, including vulnerability assessments and automated solutions, to protect sensitive data on public-facing web applications.

Fact 274: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a) mandates that businesses protect public-facing web applications against known attacks by performing vulnerability assessments or implementing automated technical solutions.

Fact 275: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107 requires businesses to protect public-facing web applications by performing vulnerability assessments or implementing automated solutions to prevent web-based attacks.

Fact 276: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171 mandates that businesses protect public-facing web applications against known attacks by conducting vulnerability assessments or implementing automated solutions.

Fact 277: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010 requires businesses to protect public-facing web applications by performing vulnerability assessments or implementing automated solutions to prevent web-based attacks.

Fact 278: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1) mandates that businesses protect public-facing web applications by conducting vulnerability assessments or implementing automated solutions to detect and prevent web-based attacks.

Fact 279: The **District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.)** mandates that businesses protect public-facing web applications by performing vulnerability assessments or implementing automated technical solutions to detect and prevent web-based attacks.

7 Requirement 7: Authorization

7.0 RESTRICT ACCESS TO CARDHOLDER DATA BY BUSINESS NEED TO KNOW

Fact 280: Federal Trade Commission Act (FTC Act), 15 U.S.C. § 45(a) prohibits unfair or deceptive practices, which include failing to restrict access to cardholder data based on business need to know, potentially leading to unauthorized access.

Fact 281: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801-6809 requires financial institutions to protect customer information by restricting access to sensitive data, such as cardholder information, based on business need to know.

Fact 282: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.308(a)(4)(i) mandates the implementation of access control policies, ensuring that access to sensitive information is limited to individuals who require it for their job functions.

Fact 283: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a) requires businesses to implement access controls that limit access to personal information, such as cardholder data, based on business need to know.

Fact 284: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107 mandates that businesses restrict access to personal information, such as cardholder data, based on business need to know to protect it from unauthorized access.

Fact 285: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171 requires businesses to restrict access to personal information, such as cardholder data, to individuals who need it for business purposes to protect it from unauthorized access.

Fact 286: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010 mandates that businesses implement access controls that limit access to personal data, such as cardholder information, based on business need to know.

Fact 287: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1) requires businesses to restrict access to consumer data, such as cardholder information, to those who need it for business purposes to protect it from unauthorized access.

Fact 288: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.) mandates that businesses limit access to personal information, such as cardholder data, based on business need to know to protect it from unauthorized access.

7.1 DEFINE ACCESS NEEDS FOR EACH ROLE AND RESTRICT ACCESS TO CARDHOLDER DATA AND SYSTEM COMPONENTS TO ONLY THOSE INDIVIDUALS WHOSE JOB REQUIRES SUCH ACCESS

Fact 289: Sarbanes-Oxley Act (SOX), 15 U.S.C. § 7262(b) requires companies to implement internal controls that define access needs for each role and restrict access to sensitive data, including cardholder information, based on job requirements.

Fact 290: Federal Trade Commission Act (FTC Act), 15 U.S.C. § 45(a) prohibits unfair or deceptive practices, including failing to define access needs and restricting access to cardholder data based on job requirements, potentially leading to unauthorized access.

Fact 291: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801-6809 mandates that financial institutions define access needs for each role and restrict access to sensitive data, such as cardholder information, to individuals whose job requires it.

Fact 292: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.308(a)(4)(i) requires the implementation of role-based access controls to ensure that access to sensitive information, such as cardholder data, is limited to individuals whose job functions require it.

Fact 293: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a) mandates that businesses define access needs for each role and restrict access to personal information, such as cardholder data, based on job requirements.

Fact 294: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107 requires businesses to define access needs and restrict access to personal information, such as cardholder data, to individuals whose job requires such access.

Fact 295: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171 mandates that businesses define access needs for each role and restrict access to personal information, such as cardholder data, based on job requirements.

Fact 296: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010 requires businesses to define access needs for each role and restrict access to personal data, such as cardholder information, based on job requirements.

Fact 297: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1) requires businesses to define access needs for each role and restrict access to consumer data, such as cardholder information, to those whose job requires it.

Fact 298: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.) mandates that businesses define access needs and restrict access to personal information, such as cardholder data, to individuals whose job requires such access.

7.2 REQUIREMENT 7.2 IMPLEMENT ACCESS CONTROL SYSTEMS THAT PROVIDE EXPLICIT APPROVAL BY AUTHORIZED PARTIES SPECIFYING REQUIRED PRIVILEGES AND ACCESS LEVELS FOR EACH INDIVIDUAL

Fact 299: Sarbanes-Oxley Act (SOX), 15 U.S.C. § 7262(b) requires companies to implement access control systems that ensure explicit approval by authorized parties for granting access privileges and specifying access levels for each individual.

Fact 300: Federal Trade Commission Act (FTC Act), 15 U.S.C. § 45(a) prohibits unfair practices, including failing to implement access control systems that require explicit

approval for granting access privileges, potentially leading to unauthorized access to cardholder data.

Fact 301: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801-6809 mandates that financial institutions implement access control systems that require explicit approval by authorized parties for granting access privileges and specifying access levels for each individual.

Fact 302: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.312(a)(1) requires the implementation of access control systems that provide explicit approval by authorized parties for granting access privileges and specifying access levels for each individual.

Fact 303: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a) mandates that businesses implement access control systems that require explicit approval by authorized parties for granting access privileges and specifying access levels for each individual.

Fact 304: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107 requires businesses to implement access control systems that ensure explicit approval by authorized parties for granting access privileges and specifying access levels for each individual.

Fact 305: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171 mandates that businesses implement access control systems that require explicit approval by authorized parties for granting access privileges and specifying access levels for each individual.

Fact 306: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010 requires businesses to implement access control systems that provide explicit approval by authorized parties for granting access privileges and specifying access levels for each individual.

Fact 307: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1) requires businesses to implement access control systems that require explicit approval by authorized parties for granting access privileges and specifying access levels for each individual.

Fact 308: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.) mandates that businesses implement access control systems that require explicit approval by authorized parties for granting access privileges and specifying access levels for each individual.

7.3 REQUIREMENT 7.3 (SECURE AND DOCUMENT ACCESS CONTROL POLICIES AND PROCEDURES)

We have no Federal, Maryland, Tennessee, Florida, Washington, California, and DC Statutes for Requirement 7.3 at this time.

8 Requirement 8: Authentication

8.0 IDENTIFY AND AUTHENTICATE ACCESS TO SYSTEM COMPONENTS

Fact 309: Federal Trade Commission Act (FTC Act), 15 U.S.C. § 45(a): Prohibits unfair or deceptive practices, including failing to identify and authenticate access to system components, potentially leading to unauthorized access to sensitive data.

Fact 310: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a): Requires businesses to establish reasonable security practices, including identification and authentication of access to personal information.

Fact 311: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107: Mandates that businesses implement identification and authentication procedures to protect personal information from unauthorized access.

Fact 312: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171(2): Requires businesses to implement policies to identify and authenticate access to personal information, ensuring protection against unauthorized access.

Fact 313: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010: Mandates that businesses establish and implement identification and authentication procedures to protect personal data from unauthorized access.

Fact 314: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1): Requires businesses to implement reasonable security procedures, including those for identification and authentication, to protect consumer data.

Fact 315: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.): Mandates that businesses implement identification and authentication procedures to protect personal information.

8.1 DEFINE AND IMPLEMENT POLICIES AND PROCEDURES TO ENSURE PROPER USER IDENTIFICATION AND AUTHENTICATION MANAGEMENT FOR NON-CONSUMER USERS AND ADMINISTRATORS ON ALL SYSTEM COMPONENTS

Fact 316: Sarbanes-Oxley Act (SOX), 15 U.S.C. § 7262(b): Requires companies to implement internal controls that define and enforce policies for user identification and authentication management, ensuring proper access controls for non-consumer users and administrators.

Fact 317: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801(b)(1): Mandates that financial institutions protect customer information by implementing and managing user identification and authentication policies.

Fact 318: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.312(a)(2)(i): Requires policies for unique user identification to protect electronic protected health information (ePHI).

8.2 IN ADDITION TO ASSIGNING A UNIQUE ID, ENSURE THAT ACCESS TO SYSTEM COMPONENTS IS AUTHENTICATED USING AT LEAST ONE OF THE FOLLOWING METHODS: SOMETHING YOU KNOW, SUCH AS A PASSWORD; SOMETHING YOU HAVE, SUCH AS A TOKEN DEVICE OR SMART CARD; SOMETHING YOU ARE, SUCH AS A BIOMETRIC

Fact 319: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.312(d): Requires the implementation of multi-factor authentication methods to verify the identity of individuals accessing electronic protected health information.

Fact 320: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1): Requires businesses to use reasonable security measures, including MFA, to protect consumer data.

Fact 321: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107: Requires businesses to implement MFA to protect personal information.

Fact 322: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171(2): Mandates the use of MFA to protect personal information from unauthorized access.

Fact 323: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010: Requires businesses to use MFA to secure access to personal data.

Fact 324: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.): Mandates that businesses use MFA to protect access to personal information.

8.3 SECURE ALL INDIVIDUAL NON-CONSOLE ADMINISTRATIVE ACCESS AND ALL REMOTE ACCESS TO THE CDE USING MULTI-FACTOR AUTHENTICATION.

Fact 325: Federal Information Security Management Act (FISMA), 44 U.S.C. § 3544(b)(2)(D)(iii): Requires federal agencies to secure non-console administrative access and remote access to sensitive systems using multi-factor authentication.

Fact 326: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801(b)(2): Requires financial institutions to protect customer information by securing remote access to the CDE with MFA.

Fact 327: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010: Requires businesses to secure remote access to personal data using MFA to prevent unauthorized access.

8.4 IMPLEMENT MULTI-FACTOR AUTHENTICATION FOR ALL ACCESS INTO THE CDE

We have no Federal, Maryland, Tennessee, Florida, Washington, California, and DC Statutes for Requirement 8.4 at this time.

8.5 DO NOT USE GROUP, SHARED, OR GENERIC IDS, PASSWORDS, OR OTHER AUTHENTICATION METHODS AS FOLLOWS: GENERIC USER IDS ARE DISABLED OR REMOVED; SHARED USER IDS DO NOT EXIST FOR SYSTEM ADMINISTRATION AND OTHER CRITICAL FUNCTIONS; SHARED AND GENERIC USER IDS ARE NOT USED TO ADMINISTER ANY SYSTEM COMPONENTS.

Fact 328: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801(b)(1): Mandates that financial institutions protect customer information by prohibiting the use of group, shared, or generic IDs and passwords to ensure that access is restricted to authorized users only. See also Requirement 2.0 regarding vendor defaults.

Fact 329: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.312(a)(2)(i): Requires the implementation of unique user identification policies to ensure that only authorized individuals have access to ePHI.

Fact 330: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a): Mandates that businesses prohibit the use of shared, generic, or vendor-supplied defaults for system passwords and IDs to protect personal information.

Florida Information Protection Act (FIPA), Fla. Stat. § 501.171(2): Requires businesses to

ensure that group, shared, or generic IDs and passwords are not used to protect personal information.

Fact 331: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.): Mandates that businesses prohibit the use of shared, generic IDs and passwords to protect personal information.

8.6 WHERE OTHER AUTHENTICATION MECHANISMS ARE USED, SUCH AS PHYSICAL OR LOGICAL SECURITY TOKENS, SMART CARDS, OR CERTIFICATES, THEY MUST BE LINKED TO AN INDIVIDUAL ACCOUNT AND ENSURE ONLY THE INTENDED ACCOUNT CAN USE THAT MECHANISM

Fact 332: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.312(a)(2)(i): Requires the implementation of authentication mechanisms that are linked to individual accounts to ensure only authorized individuals can access electronic protected health information.

Fact 333: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801(b)(2): Requires that authentication mechanisms, such as tokens or smart cards, are linked to individual accounts to protect customer information.

Fact 334: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1): Requires businesses to ensure that authentication mechanisms are securely linked to individual accounts to protect consumer data.

9 Requirement 9: Physical Security

9.0 RESTRICT PHYSICAL ACCESS TO CARDHOLDER DATA

Fact 335: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.310(a)(1): Requires the implementation of policies and procedures to limit physical access to electronic information systems and the facilities in which they are housed to authorized individuals.

Fact 336: Federal Trade Commission Act (FTC Act), 15 U.S.C. § 45(a): Prohibits unfair or deceptive practices, which can include failing to restrict physical access to cardholder data, potentially leading to unauthorized access to sensitive data.

Fact 337: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a): Requires businesses to establish and maintain reasonable security procedures to restrict physical access to personal information.

Fact 338: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107: Mandates that businesses restrict physical access to facilities where personal information is stored to protect it from unauthorized access.

Fact 339: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171(2): Requires businesses to implement physical security measures to restrict access to areas where personal information is stored.

Fact 340: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010: Requires businesses to restrict physical access to facilities containing personal data to protect against unauthorized access.

Fact 341: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1): Mandates that businesses implement reasonable security procedures, including physical access restrictions, to protect consumer data.

Fact 342: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.): Requires businesses to restrict physical access to personal information to protect it from unauthorized access.

9.1 USE APPROPRIATE FACILITY ENTRY CONTROLS TO LIMIT AND MONITOR PHYSICAL ACCESS TO SYSTEMS IN THE CARDHOLDER DATA ENVIRONMENT

Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.310(a)(2)(ii): Requires the implementation of facility security controls to limit physical access to systems housing electronic protected health information (ePHI).

Federal Information Security Management Act (FISMA), 44 U.S.C. § 3544(b)(2)(D)(iv): Requires federal agencies to implement physical access controls to secure sensitive systems and data.

Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a): Requires businesses to use facility security controls to limit access to areas where personal information is stored.

Fact 343: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171(2): Mandates the use of appropriate facility entry controls to limit and monitor physical access to systems containing personal information.

Fact 344: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010: Requires businesses to implement facility entry controls to monitor and limit access to areas containing personal data.

Fact 345: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1): Requires businesses to implement reasonable security procedures, including facility entry controls, to protect consumer data.

Fact 346: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.): Mandates that businesses use facility entry controls to limit and monitor physical access to personal information.

9.2 DEVELOP PROCEDURES TO DISTINGUISH BETWEEN ONSITE PERSONNEL AND VISITORS AND CONTROL VISITOR ACCESS TO THE CARDHOLDER DATA ENVIRONMENT

Fact 347: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.310(b): Requires the implementation of policies and procedures to control and monitor visitor access to facilities housing electronic protected health information (ePHI).

Fact 348: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801(b)(2): Requires financial institutions to implement procedures for controlling visitor access to areas where customer information is stored.

Fact 349: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a): Mandates that businesses develop and enforce procedures to distinguish between onsite personnel and visitors and to control visitor access to facilities containing personal information.

Fact 350: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171(2): Requires businesses to implement procedures to control visitor access to areas where personal information is stored, distinguishing between personnel and visitors.

Fact 351: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010: Requires businesses to establish procedures to control visitor access to facilities containing personal data and to distinguish between personnel and visitors.

Fact 352: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1): Mandates that businesses implement procedures to control visitor access to areas where consumer data is stored.

Fact 353: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.): Requires businesses to control visitor access to facilities housing personal information and to distinguish between personnel and visitors.

9.3 CONTROL PHYSICAL ACCESS FOR ONSITE PERSONNEL TO THE CARDHOLDER DATA ENVIRONMENT

Fact 354: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.310(a)(2)(iii): Requires the implementation of physical access controls for onsite personnel to areas housing electronic protected health information (ePHI).

Fact 355: Sarbanes-Oxley Act (SOX), 15 U.S.C. § 7262(b): Requires companies to implement internal controls, including physical access controls, to secure areas containing sensitive financial data.

Fact 356: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801(b)(2): Mandates that financial institutions control physical access for onsite personnel to areas where customer information is stored.

Fact 357: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a): Requires businesses to control physical access for onsite personnel to areas where personal information is stored.

Fact 358: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171(2): Mandates that businesses control physical access for onsite personnel to areas containing personal information.

Fact 359: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010: Requires businesses to control physical access for onsite personnel to facilities containing personal data.

Fact 360: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1): Requires businesses to control physical access for onsite personnel to areas where consumer data is stored.

Fact 361: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.): Mandates that businesses control physical access for onsite personnel to areas containing personal information.

9.4 WE HAVE NO FEDERAL, MARYLAND, TENNESSEE, FLORIDA, WASHINGTON, CALIFORNIA, AND DC STATUTES FOR REQUIREMENT 9.4 AT THIS TIME.

9.5 PHYSICALLY SECURE ALL MEDIA CONTAINING CARDHOLDER DATA

Fact 362: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.310(d)(1): Requires the implementation of policies and procedures to physically secure media containing electronic protected health information (ePHI).

Fact 363: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801(b)(2): Mandates that financial institutions physically secure all media containing customer information.

Fact 364: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a): Requires businesses to secure all media containing personal information physically.

Fact 365: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107: Mandates that businesses physically secure all media containing personal information.

Fact 366: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171(2): Requires businesses to physically secure all media containing personal information.

Fact 367: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010: Mandates that businesses physically secure all media containing personal data.

Fact 368: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1): Requires businesses to secure all media containing consumer data physically.

Fact 369: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.): Mandates that businesses physically secure all media containing personal information.

9.6 MAINTAIN STRICT CONTROL OVER THE INTERNAL OR EXTERNAL DISTRIBUTION OF ANY KIND OF MEDIA THAT CONTAINS CARDHOLDER DATA

Fact 370: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.310(d)(2)(i): Requires the implementation of policies and procedures to control the movement and distribution of media containing electronic protected health information (ePHI).

Fact 371: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801(b)(2): Mandates that financial institutions maintain control over the internal and external distribution of media containing customer information.

Fact 372: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a): Requires businesses to maintain control over the distribution of media containing personal information.

Fact 373: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107: Mandates that businesses control the internal and external distribution of media containing personal information.

Fact 374: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171(2): Requires businesses to maintain control over the internal and external distribution of media containing personal information.

Fact 375: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010: Requires businesses to control the distribution of media containing personal data.

Fact 376: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1): Mandates that businesses maintain strict control over the distribution of media containing consumer data.

Fact 377: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.): Requires businesses to control the internal and external distribution of media containing personal information.

9.7 ENSURE MANAGEMENT APPROVES ANY AND ALL MEDIA CONTAINING CARDHOLDER DATA THAT IS MOVED FROM A SECURED AREA, INCLUDING WHEN MEDIA IS DISTRIBUTED TO INDIVIDUALS

Fact 378: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.310(d)(2)(ii): Requires management approval for the movement of media containing electronic protected health information (ePHI) from secured areas.

Fact 379: Gramm**-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801(b)(2):** Mandates that financial institutions require management approval for the movement of media containing customer information from secured areas.

Fact 380: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a): Requires management approval for the movement of media containing personal information from secured areas.

Fact 381: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107: Mandates that businesses obtain management approval before moving media containing personal information from secured areas.

Fact 382: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171(2): Requires businesses to ensure that management approves the movement of media containing personal information from secured areas.

Fact 383: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010: Requires management approval for the movement of media containing personal data from secured areas.

Fact 384: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1): Mandates that businesses obtain management approval before moving media containing consumer data from secured areas.

Fact 385: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.): Requires management approval for the movement of media containing personal information from secured areas.

9.8 SECURELY STORE MEDIA CONTAINING CARDHOLDER DATA AND PROTECT IT FROM UNAUTHORIZED ACCESS.

Fact 386: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.310(d)(1): Requires the implementation of policies and procedures to securely store media containing electronic protected health information (ePHI) and protect it from unauthorized access.

Fact 387: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801(b)(2): Mandates that financial institutions securely store media containing customer information and protect it from unauthorized access.

Fact 388: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a): Requires businesses to securely store media containing personal information and protect it from unauthorized access.

Fact 389: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107: Mandates that businesses securely store media containing personal information and protect it from unauthorized access.

Fact 390: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171(2): Requires businesses to securely store media containing personal information and protect it from unauthorized access.

Fact 391: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010: Requires businesses to securely store media containing personal data and protect it from unauthorized access.

Fact 392: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1): Mandates that businesses securely store media containing consumer data and protect it from unauthorized access.

Fact 393: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.): Requires businesses to securely store media containing personal information and protect it from unauthorized access.

9.9 MAINTAIN STRICT CONTROL OVER THE STORAGE AND ACCESSIBILITY OF MEDIA CONTAINING CARDHOLDER DATA, ENSURING IT IS DESTROYED WHEN NO LONGER NEEDED

Fact 394: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.310(d)(2)(ii): Requires the implementation of policies and procedures to maintain control over the storage and accessibility of media containing electronic protected health information (ePHI) and ensure it is destroyed when no longer needed.

Fact 395: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801(b)(2): Mandates that financial institutions maintain strict control over the storage and accessibility of media containing customer information, ensuring it is destroyed when no longer needed.

Fact 396: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a): Requires businesses to maintain control over the storage and accessibility of media containing personal information and ensure it is destroyed when no longer needed.

Fact 397: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107: Mandates that businesses control the storage and accessibility of media containing personal information, ensuring it is destroyed when no longer needed.

Fact 398: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171(2): Requires businesses to maintain control over the storage and accessibility of media containing personal information and ensure it is destroyed when no longer needed.

Fact 399: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010: Requires businesses to control the storage and accessibility of media containing personal data, ensuring it is destroyed when no longer needed.

Fact 400: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1): Mandates that businesses maintain control over the storage and accessibility of media containing consumer data, ensuring it is destroyed when no longer needed.

Fact 401: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.): Requires businesses to control the storage and accessibility of media containing personal information, ensuring it is destroyed when no longer needed.

9.10 ENSURE THAT ALL MEDIA CONTAINING CARDHOLDER DATA IS SECURELY ERASED, RENDERED UNREADABLE, OR PHYSICALLY DESTROYED WHEN NO LONGER NEEDED.

Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.310(d)(2)(ii): Requires the secure erasure, rendering unreadable, or physical destruction of media containing electronic protected health information (ePHI) when no longer needed.

Fact 402: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801(b)(2): Mandates that financial institutions securely erase, render unreadable, or physically destroy media containing customer information when no longer needed.

Fact 403: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a): Requires businesses to securely erase, render unreadable, or physically destroy media containing personal information when no longer needed.

Fact 404: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107: Mandates that businesses securely erase, render unreadable, or physically destroy media containing personal information when no longer needed.

Fact 405: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171(2): Requires businesses to securely erase, render unreadable, or physically destroy media containing personal information when no longer needed.

Fact 406: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010: Requires businesses to securely erase, render unreadable, or physically destroy media containing personal data when no longer needed.

Fact 407: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1): Mandates that businesses securely erase, render unreadable, or physically destroy media containing consumer data when no longer needed.

Fact 408: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.): Requires businesses to securely erase, render unreadable, or physically destroy media containing personal information when no longer needed.

10 Requirement 10: Access Logging and Monitoring

10.0 Implement Audit Controls to Track Access

Fact 409: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.312(b): Requires the implementation of audit controls to record and examine access to electronic protected health information (ePHI).

Fact 410: Federal Trade Commission Act (FTC Act), 15 U.S.C. § 45(a): Prohibits unfair or deceptive practices, including failing to track and monitor access to network resources and cardholder data, potentially leading to unauthorized access to sensitive data.

Fact 411: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a): Requires businesses to establish security practices, including tracking and monitoring access to personal information.

Fact 412: Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. § 47-18-2107: Requires businesses to implement tracking and monitoring of access to personal information to prevent unauthorized access.

Fact 413: Florida Information Protection Act (FIPA), Fla. Stat. § 501.171(2): Mandates businesses to monitor access to personal information to ensure it is protected from unauthorized access.

Fact 414: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010: Requires businesses to track and monitor access to personal data.

Fact 415: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1): Requires businesses to monitor and track access to consumer data.

Fact 416: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.): Mandates businesses to track and monitor access to personal information.

10.1 IMPLEMENT AUTOMATED AUDIT TRAILS FOR SYSTEM COMPONENTS

Fact 417: Sarbanes-Oxley Act (SOX), 15 U.S.C. § 7262(b): Mandates the implementation of internal controls and audit trails to reconstruct events related to access to financial data.

Fact 418: Federal Information Security Management Act (FISMA), 44 U.S.C. § 3544(b)(2)(D)(ii): Requires federal agencies to implement audit trails to monitor and reconstruct events related to access to sensitive systems and data.

Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801(b)(2): Requires financial institutions to implement automated audit trails to reconstruct events related to access to customer information.

Florida Information Protection Act (FIPA), Fla. Stat. § 501.171(2): Mandates that businesses implement automated audit trails to reconstruct events related to access to personal information.

California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1): Requires businesses to implement audit trails to track and reconstruct events related to access to consumer data.

10.2 RECORD AUDIT TRAIL ENTRIES FOR USER IDENTIFICATION AND EVENTS

Fact 419: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.312(b): Requires the recording of specific audit trail entries, including user identification, type of event, date and time, and other relevant details for access to electronic protected health information (ePHI).

Fact 420: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a): Requires businesses to record specific audit trail entries for access to personal information.

Fact 421: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010: Requires businesses to record specific audit trail entries for access to personal data.

10.3 ENSURE CENTRALIZED LOGGING OF AUDIT TRAILS

Fact 422: Federal Information Security Management Act (FISMA), 44 U.S.C. § 3544(b)(2)(D)(ii): Requires federal agencies to ensure audit trails are sent to a centralized logging system that is difficult to alter.

Fact 423: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1): Requires businesses to store audit trails in a centralized logging system or media that is difficult to alter.

10.4 REVIEW LOGS DAILY AND RETAIN AUDIT TRAIL ENTRIES FOR ONE YEAR

Fact 424: Sarbanes-Oxley Act (SOX), 15 U.S.C. § 7262(b): Mandates the daily review of logs and the retention of audit trail entries for at least one year to monitor access to financial data.

Fact 425: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801(b)(2): Requires financial institutions to review logs daily and retain audit trail entries for at least one year.

Fact 426: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1): Requires businesses to review logs daily and retain audit trail entries for at least one year.

10.5 USE FILE INTEGRITY MONITORING OR CHANGE DETECTION SOFTWARE

Fact 427: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.312(c)(1): Requires the implementation of file integrity monitoring or change detection software to ensure that existing log data cannot be altered without generating alerts, protecting the integrity of logs related to electronic protected health information (ePHI).

Fact 428: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a): Requires businesses to use file integrity monitoring or change detection software on logs.

Fact 429: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010: Requires businesses to use file integrity monitoring or change detection software on logs.

10.6 PROTECT LOG DATA AGAINST UNAUTHORIZED ACCESS

Fact 430: Sarbanes-Oxley Act (SOX), 15 U.S.C. § 7262(b): Mandates the implementation of access controls to protect log data against unauthorized access, securing financial data.

10.7 REVIEW AND MANAGE ACCESS TO AUDIT TRAILS

Fact 431: District of Columbia Consumer Protection Procedures Act (D.C. Code § 28-3851 et seq.): Mandates that businesses manage access to audit trails, ensuring that only authorized personnel have access.

10.8 ENSURE AUDIT TRAIL INTEGRITY

Fact 432: We have no Federal, Maryland, Tennessee, Florida, Washington, California, and DC Statutes for Requirement 10.8 at this time.

10.9 MAINTAIN LOG DATA SECURITY

Fact 433: We have no Federal, Maryland, Tennessee, Florida, Washington, California, and DC Statutes for Requirement 10.9 at this time.

11 Requirement 11: Testing and Remediation

11.0 CONDUCT VULNERABILITY SCANNING AND PENETRATION TESTING

Fact 434: Federal Information Security Management Act (FISMA), 44 U.S.C. § 3544(b)(8): Requires federal agencies to regularly test security systems and processes through vulnerability scanning and penetration testing to identify and address vulnerabilities.

Fact 435: Maryland Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503(a): Requires businesses to implement security practices, including regular vulnerability scanning and penetration testing to protect personal information.

Fact 436: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1): Requires businesses to test their security systems to protect consumer data regularly.

Fact 437: Washington Data Breach Notification Law, Rev. Code Wash. (RCW) § 19.255.010: Mandates that businesses regularly test security systems and processes to prevent unauthorized access to personal data.

11.1 IMPLEMENT NETWORK INTRUSION DETECTION SYSTEMS (IDS) AND PREVENTION SYSTEMS (IPS)

Fact 438: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.312(c)(1): Requires the implementation of security measures, including IDS/IPS, to protect against malicious software and unauthorized access to electronic protected health information (ePHI).

Fact 439: Sarbanes-Oxley Act (SOX), 15 U.S.C. § 7262(b): Mandates internal controls, including network intrusion detection and prevention systems, to secure financial data.

11.2 REGULARLY TEST SECURITY CONTROLS

Fact 440: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801(b)(2): Requires financial institutions to regularly test their security controls to ensure they are effective in protecting customer information.

Fact 441: Federal Information Security Management Act (FISMA), 44 U.S.C. § 3544(b)(9): Requires regular testing of security controls for federal information systems.

11.3 MONITOR AND ANALYZE SECURITY ALERTS AND LOGS

Fact 442: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.308(a)(6)(ii): Requires the monitoring and analysis of security alerts and logs to identify and respond to security incidents involving electronic protected health information (ePHI).

Fact 443: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801(b)(2): Mandates that financial institutions monitor and analyze security alerts and logs to detect unauthorized access to customer information.

11.4 VERIFY THAT PHYSICAL SECURITY CONTROLS ARE IN PLACE AND EFFECTIVE

Fact 444: Sarbanes-Oxley Act (SOX), 15 U.S.C. § 7262(b): Requires regular verification of physical security controls to protect financial data from unauthorized access.

Fact 445: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.310(c): Mandates the implementation and regular verification of physical security controls to safeguard electronic protected health information (ePHI).

11.5 IMPLEMENT CHANGE DETECTION SOFTWARE TO ALERT PERSONNEL TO UNAUTHORIZED MODIFICATIONS

Fact 446: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.312(c)(2): Requires the implementation of change detection software to alert personnel to unauthorized modifications to electronic protected health information (ePHI).

11.6 ENSURE LOGGING MECHANISMS ARE PROTECTED FROM UNAUTHORIZED ACCESS

Fact 447: Sarbanes-Oxley Act (SOX), 15 U.S.C. § 7262(b): Mandates the implementation of controls to protect logging mechanisms from unauthorized access to secure financial data.

11.7 CONDUCT REGULAR SECURITY ASSESSMENTS

Fact 448: We have no Federal, Maryland, Tennessee, Florida, Washington, California, and DC Statutes for Requirement 11.7 at this time.

11.8 IMPLEMENT PROCEDURES FOR IDENTIFYING AND RESPONDING TO SECURITY INCIDENTS

Fact 449: We have no Federal, Maryland, Tennessee, Florida, Washington, California, and DC Statutes for Requirement 11.8 at this time.

12 Requirement 12: Policy Management

12.0 Develop and Maintain a Security Policy

Fact 450: Federal Information Security Management Act (FISMA), 44 U.S.C. § 3544(b)(2)(D): Requires federal agencies to develop, document, and implement an information security program, which includes maintaining a security policy to protect information systems.

Fact 451: Sarbanes-Oxley Act (SOX), 15 U.S.C. § 7262(b): Mandates the implementation of internal controls, including maintaining a policy that addresses information security for financial data.

Fact 452: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.308(a)(1): Requires covered entities to implement policies and procedures to ensure the security of electronic protected health information (ePHI).

12.1 Implement an Acceptable Use Policy for Information Systems

Fact 453: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801(b)(1): Requires financial institutions to develop, implement, and maintain an acceptable use policy to ensure the security and confidentiality of customer information.

Fact 454: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.308(a)(3): Mandates the implementation of policies for acceptable use of information systems that access electronic protected health information (ePHI).

12.2 ESTABLISH PROCEDURES TO HANDLE SECURITY INCIDENTS

Fact 455: Federal Information Security Management Act (FISMA), 44 U.S.C. § 3544(b)(7): Requires federal agencies to establish procedures for detecting, reporting, and responding to security incidents involving federal information systems.

Fact 456: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.308(a)(6): Requires the implementation of procedures to address security incidents related to electronic protected health information (ePHI).

Fact 457: California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1): Requires businesses to establish procedures to identify and respond to security incidents involving consumer data.

12.3 DEVELOP A RISK MANAGEMENT PROGRAM

Fact 458: Sarbanes-Oxley Act (SOX), 15 U.S.C. § 7262(b): Mandates the development and implementation of a risk management program to protect financial data from security threats.

Fact 459: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801(b)(2): Requires financial institutions to establish a risk management program to safeguard customer information.

Fact 460: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.308(a)(1)(ii)(A): Requires covered entities to conduct a risk analysis as part of their security management process for electronic protected health information (ePHI).

12.4 DEFINE AND COMMUNICATE SECURITY RESPONSIBILITIES FOR PERSONNEL

Fact 461: Federal Information Security Management Act (FISMA), 44 U.S.C. § 3544(a)(3)(D): Requires federal agencies to define and communicate security responsibilities to all personnel involved in the management and security of federal information systems.

Fact 462: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.308(a)(2): Mandates that covered entities assign security responsibilities to personnel involved in the handling of electronic protected health information (ePHI).

12.5 ESTABLISH AND DOCUMENT A SECURITY AWARENESS PROGRAM

Fact 463: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801(b)(2): Requires financial institutions to develop and document a security awareness program to educate employees about information security.

Fact 464: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.308(a)(5)(i): Requires covered entities to implement a security awareness and training program for all workforce members involved in the handling of electronic protected health information (ePHI).

Fact 465: Federal Information Security Management Act (FISMA), 44 U.S.C. § 3544(b)(4): Requires federal agencies to establish and document a security awareness program for personnel managing federal information systems.

12.6 IMPLEMENT A PROCESS FOR MONITORING AND EVALUATING SECURITY POLICIES

Fact 466: Sarbanes-Oxley Act (SOX), 15 U.S.C. § 7262(b): Requires the continuous monitoring and evaluation of security policies and controls to protect financial data.

Fact 467: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801(b)(2): Mandates that financial institutions implement a process for regularly monitoring and evaluating the effectiveness of their security policies.

Fact 468: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.308(a)(8): Requires regular evaluations of the security policies in place to protect electronic protected health information (ePHI).

12.7 MAINTAIN AN INCIDENT RESPONSE PLAN

Fact 469: Federal Information Security Management Act (FISMA), 44 U.S.C. § 3544(b)(7): Requires federal agencies to maintain an incident response plan to address security breaches involving federal information systems.

Fact 470: Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.308(a)(6)(i): Mandates that covered entities maintain an incident response plan to handle security incidents involving electronic protected health information (ePHI).

12.8 MAINTAIN THIRD-PARTY SECURITY POLICIES

Fact 471: We have no Federal, Maryland, Tennessee, Florida, Washington, California, and DC Statutes for Requirement 12.8 at this time.

12.9 IMPLEMENT POLICIES FOR SECURING PHYSICAL MEDIA

Fact 472: We have no Federal, Maryland, Tennessee, Florida, Washington, California, and DC Statutes for Requirement 12.9 at this time.

D Operational Necessity

1 Course of Dealing

Fact 473: Since 2021, Ryan Dillon-Capps has served as the PCI Compliance Officer for Ohana Growth Partners. The Defense is providing the first three pages of the last nineteen PCI Scan Summary Reports, covering the period from July 2022 to May 2024. These reports consistently list Dillon-Capps as the PCI Compliance Officer, in the top left corner of page 2 of each report. The compliance status is marked as "Pass" on the bottom left corner of page 3.

Ex. 10R: PCI Scan Summary Reports (July 2022 - May 2024), pp. 2-3, 5-6, 8-9, 11-12, 14-15, 17-18, 20-21, 23-24, 26-27, 29-30, 32-33, 35-36, 38-39, 41-42, 44-45, 47-48, 50-51, 53-54, 56-57.

Fact 474: Dillon-Capps's role as PCI Compliance Officer extends across all departments, vendors, and executives. Holding authority over access controls, standards, policies, and training requirements to ensure the implementation of administrative, technical, and physical safeguards for PCI Compliance. Ensuring that Ohana remains compliant with state and federal laws**.**

[Ex. 10B at 1; Exhibit 10F at 2-3; Exhibit 10K at 1-2; Exhibit 22F-1; Exhibit 22H-1; Exhibit 22H-2]

Fact 475: PCI DSS v4 Requirement 12 requires defined policies, and Exhibit 22H-2, p.2-3, § 8-10 is Ohana Growth Partners' IT Terms and Use Policy v2 that reflects the company policies related to Requirement 2, 6, 7, and 10.

Fact 476: Everyone who uses the Microsoft Cloud environment signs the IT Terms and Use Policy, regardless of their position within the organization. **[Exhibit 22H-1, p.1]**

2 Contractual Obligations

Fact 477: Ohana has stated that they are unaware of the basis for incurring a PCI compliance violation when authorizing access without any information about the individual's job or assigned tasks. This admission highlights a significant liability for the organization, demonstrating the necessity for the plaintiff to comply with the defendant's authority as PCI Compliance Officer.

[Ex. 9C ¶16; Ex. 10Q; Ex. 10W; Ex. 10X]

Fact 478: Ohana is a Planet Fitness franchisee that operates in five states and the District of Columbia. The Franchise Disclosure Documents (FDD) are regulated by the FTC and local state authorities, requiring Ohana to sign at least six different FDDs.

[Ex. 9A-1 ¶7; Ex. 10S; Ex. 10T; Ex. 10U; Ex. 10V]

Fact 479: Each of the Franchise Disclosure Documents (FDDs) includes an addendum to the Master Service Agreement (MSA) from the processor, which extends the obligations, liabilities, and duties of Planet Fitness, as the merchant, to the franchisee, Ohana. The agreement specifies that "each party confirms that it is, and shall be, in full compliance... with all laws, statutes and federal and state regulations, as well as rules and operating regulations and bylaws imposed by Visa/MasterCard/Discover" and that "Merchant hereby certifies that it... complies with the Payment Card Industry ('PCI') standards instituted by Visa/MasterCard/Discover." **[Ex. 10P, p.21, §3.10]**

Fact 480: The consistent adherence to compliance standards under the guidance of Ryan Dillon-Capps has historically ensured compliance with PCI DSS and relevant federal laws, effectively mitigating the risk of data breaches and other security incidents. Any deviation from

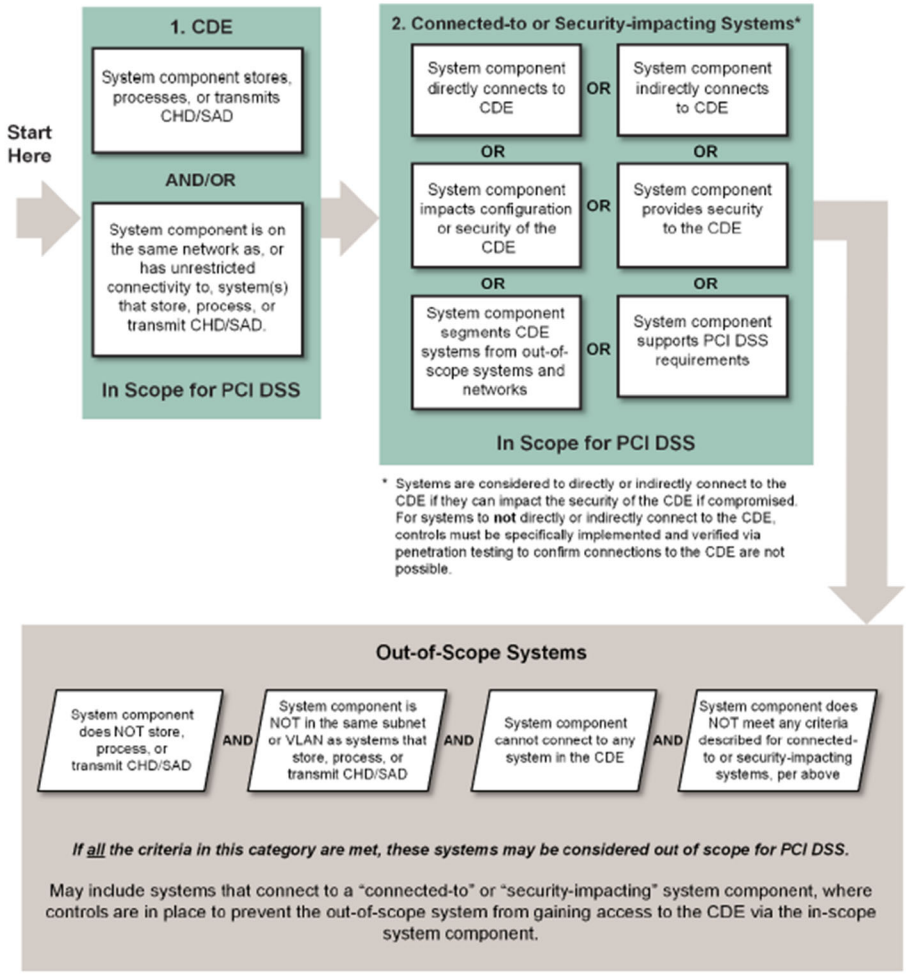
these practices, including the Plaintiff's failure to follow Dillon-Capps' guidance, introduces significant risks of non-compliance, potentially leading to legal and financial repercussions for Ohana Growth Partners. **[Ex. 10F; Ex. 10K]**

3 PCI DSS Scoping

Fact 481: PCI DSS requirements apply to the cardholder data environment (CDE), which includes system components, people, and processes that store, process, or transmit cardholder data or sensitive authentication data. These requirements can extend even to entities that do not handle PANs (Primary Account Numbers) if they can impact the security of the CDE. The concept of "in-scope" means that any system connected to the CDE must also comply with PCI DSS standards. The figure below illustrates this chain of connectivity, highlighting that everything capable of connecting to any system in the CDE is considered in scope. **[Ex. 22A-13 pp 1, 3]**

Figure 1 shows considerations for scoping system components for PCI DSS.

Figure 1. Understanding PCI DSS Scoping



4 iPads

Fact 482: Prospects and members use company-owned iPads to access a secure webpage where they input their payment information. Under PCI DSS v4, the transmission of payment card information requires that both the iPads and the network they use be PCI compliant. Additionally, any system that can affect the security of devices that transmit, process, or store payment information must also maintain PCI compliance. This includes the

mobile device management (MDM) solution called Intune and the access management system called Entra ID. Secured Network Requirement 1 is provided as **Ex. 22A-1;** Secured Data Requirement 3 is provided as **Ex. 22A-3**

5 Intune – Mobile Device Management (MDM)

Fact 483: Intune provides centralized management of the iPads as required under Change Control Management Requirement 6 **[Ex. 22A-6].** This is part of managing the authentication requirements under Authentication Requirement 8 **[Ex. 22A-8].**

6 Entra ID

Fact 484: Entra ID provides authentication controls required under Authentication Requirement 8, provided as **Ex.22A-8**, and is the mechanism by which we implement Authorization Requirement 7, provided as **Ex.22A-7**, and is configured with storage solutions to track and monitor access to Intune and other systems as required under Access Logging and Monitoring Requirement 10, provided as **Ex. 22A-10**.

7 iPad Kiosk Platform

Fact 485: The iPad Kiosk platform is hosted in the Microsoft Cloud environment and was designed to reproduce the individual club-specific webpage appearance while implementing functionality to add, remove, edit, and centrally manage all the clubs and their kiosk webpages through the secure and cost-effective platform.

Fact 486: Developers who create software that exists within this card data environment (CDE) must complete annual training to validate that they are capable of producing secure code and are following the current best practices. Secure Coding and vulnerability management

practices under Requirements 6 and authentication controls under Requirement 8 are provided as **Ex. 22A-6** and **Ex. 22-8**.

E Regulatory and Judicial Penalties

Fact 487: Regulatory fines and penalties for non-compliance with data protection laws can lead to significant financial consequences. For instance, violations of the Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. § 6805(a), which mandates the protection of consumer financial data, can result in penalties of up to $100,000 per violation for institutions and $10,000 for officers involved in certain willful violations. Additionally, severe criminal penalties, including fines and imprisonment, can result from violations involving unauthorized access or intentional misconduct under statutes like the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030(c).

Fact 488: Civil litigation from data breaches frequently triggers class-action lawsuits. In the **Equifax Data Breach of 2017**, which exposed the personal information of 147 million people, the company faced numerous lawsuits leading to a global settlement of up to $700 million (**FTC v. Equifax Inc., No. 1:19-cv-03297-TWT, 2019 WL 3802067 (N.D. Ga. 2019)**).

Fact 489: The Federal Trade Commission (FTC) has broad authority to enforce data security under the FTC Act. In **FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015)**, the court upheld the FTC's ability to bring enforcement actions against companies for failing to implement adequate cybersecurity measures, resulting in significant fines and mandatory corrective actions.

Fact 490: Data breaches can lead to substantial direct financial losses, including the costs of forensic investigations, legal fees, and compensation for affected individuals. For example, the **Home Depot Data Breach in 2014** resulted in a total expenditure of $161 million in breach-related costs, including legal fees and settlements (**In re Home Depot, Inc., Customer Data Security Breach Litigation, No. 1:14-md-02583-TWT, 2016 WL 6902351 (N.D. Ga. 2016)**).

Fact 491: Following a data breach, organizations often incur increased costs to enhance their cybersecurity measures to meet regulatory requirements. This may involve upgrading systems, hiring additional IT staff, and implementing more rigorous monitoring and auditing processes. For example, after the Target Data Breach, the company reportedly spent significant amounts on security upgrades and related expenses, with costs estimated to be over $202 million (as per Target's financial reports).

Fact 492: Organizations typically must offer credit monitoring services to affected individuals, adding to the financial burden. For instance, **Equifax** set aside up to $425 million to help those affected by its breach (**FTC v. Equifax Inc., No. 1:19-cv-03297-TWT, 2019 WL 3802067 (N.D. Ga. 2019)**.

Fact 493: A data breach can halt key business operations, especially those involving point-of-sale (POS) systems and online transactions. The Sony PlayStation Network outage in 2011 lasted 23 days and cost the company an estimated $171 million in lost revenue and remediation efforts (as reported in Sony's official statements and financial disclosures).

Fact 494: Following a breach, organizations may be subjected to rigorous compliance audits and increased scrutiny from regulators, diverting resources from regular business activities.

Fact 495: A data breach can severely damage an organization's reputation, leading to a loss of customer trust. Following the Target Data Breach, the company experienced a significant drop in sales, with a reported 46% decrease in profits in the fourth quarter of 2013, as consumers feared for the security of their personal information (according to Target's financial reports and earnings statements).

Fact 496: Publicly traded companies often see their stock prices drop following a major data breach. The **Equifax Data Breach** led to a significant decline in its stock price, reflecting the market's reaction to the loss of consumer confidence and anticipated legal liabilities (**FTC v. Equifax Inc., No. 1:19-cv-03297-TWT, 2019 WL 3802067 (N.D. Ga. 2019)**).

Fact 497: In cases where data breaches result from willful misconduct or intentional disregard for data security, particularly involving unauthorized access or exceeding authorized access, individuals may face criminal charges under statutes like the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030(c). While PCI DSS non-compliance itself may not directly lead to CFAA charges, significant failures in protecting systems can result in legal consequences for responsible parties.

Fact 498: Corporate executives could face consequences for failures in cybersecurity governance under laws like the Sarbanes-Oxley Act (SOX), particularly if they knowingly misrepresent or fail to disclose material information. In the case of the Yahoo Data Breach, the

company faced SEC charges for failing to properly disclose the breach to investors in a timely manner. Yahoo agreed to a $35 million settlement with the SEC (Securities and Exchange Commission Release No. 83065 / April 24, 2018).

Fact 499: The unmitigated risks of non-compliance with PCI DSS and related data protection statutes are severe and multifaceted. They encompass significant legal liabilities, financial costs, operational disruptions, reputational damage, and potential criminal prosecution. The interconnectedness of these risks underlines the critical importance of rigorous adherence to PCI DSS standards and other legal obligations concerning data security.

III CONTEXT

A Context of PCI DSS

Fact 500: The context of PCI DSS (Payment Card Industry Data Security Standard) is fundamentally connected to the ethical obligation and industry mandates to protect the public interest by safeguarding consumer financial data. As the prevalence of electronic payment systems grew, so did the risk of data breaches and financial fraud, posing significant threats not only to businesses but also to the public at large.

Fact 501: Driving Forces: **Driving Forces:** The primary driving forces behind the establishment of PCI DSS were the necessity to protect consumers' sensitive financial information, the industry's responsibility to prevent data breaches, and the broader public interest in maintaining trust in the financial system. Aligning with data protection laws and mitigating the legal consequences of failing to secure payment data also played crucial roles in shaping the standard

Fact 502: Background: Recognizing the significant risks to consumers and the potential for widespread harm, major credit card companies collaborated in 2004 to create PCI DSS. This standard was developed as a **proactive measure** to establish a unified approach to data security, reflecting both industry best practices and the need to meet regulatory and legal expectations

Fact 503: Purpose and Goals: The purpose of PCI DSS is to ensure that entities handling payment card information implement robust security measures to protect that data from unauthorized access and misuse. This aligns with the public interest by reducing the risk of financial loss, identity theft, and erosion of consumer confidence in the payment card system.

Fact 504: Specifics: PCI DSS outlines a comprehensive set of requirements that organizations must follow, covering areas such as network security, encryption, access control, and continuous monitoring. Compliance with these standards is not only a business imperative but also a contractual expectation, as failure to protect cardholder data can result in severe legal penalties under data protection laws, reputational damage, and a breach of public trust.

Fact 505: In summary, the context of PCI DSS is deeply rooted in the commitment to protect the public interest by ensuring the security of payment card data, thereby upholding consumer trust and preventing the far-reaching consequences of data breaches and financial fraud. While not a legal requirement in itself, PCI DSS helps organizations meet their legal obligations under data protection laws.

B Segregation of Duties (SoD)

Fact 506: "Authorized Personnel" refers to individuals who are either responsible for protecting the CDE or can impact its security, as well as the security of sensitive authentication data. This term encompasses those actively involved in maintaining PCI compliance. Only Authorized Personnel responsible for access management can grant access. **[Ex. 22A-15; Ex. 22A-7]**

Fact 507: Authorized Custodians" are personnel responsible for managing cryptographic keys and other critical access components. This role relates to the principle of Segregation of Duties (SoD), which involves distributing responsibilities among multiple individuals to enhance security. In larger organizations, SoD is often implemented naturally through least privileged access. In smaller organizations, additional measures may be necessary to prevent access from becoming concentrated. Examples of roles include Viva Goals Administrator, Billing Administrator, and User Administrators. **[Ex. 22A-16 at 1;Ex. 5C; Ex. 6F; Ex. 6G; Ex. 24K]**

Fact 508: Ryan Dillon-Capps created an account for Geoff VanMaastrich with the Global Administrator role, but VanMaastrich declined. Karen Cepress and Ronaldo Pedraza were in discussions to receive accounts with the same role. Justin Drummond agreed to receive an account with the Global Administrator Role on June 7, 2024, but requested to delay the receipt of the account on June 11, 2024. [**Ex. 1I; Ex. 1T]**

Fact 509: Dillon-Capps provided additional access to the HR Training Department on May 30, 2024, and the Help Desk as part of ongoing efforts to distribute access and prepare to implement Privileged Identity Management. (PIM)

Fact 510: Microsoft recommended the company Finchloom to support Ohana's cloud environment, and between May 20 and June 13. The Defendant requested the support from Finchloom or other qualified Microsoft cloud experts. Glenn Norris refused to bring anyone until Hartman Executive Advisors misrepresented themself before refusing to respond to numerous attempts by Dillon-Capps to contact them and provide them access.

Fact 511: The purpose of an access control model is to standardize the assignment of access rights, reducing errors like granting excessive privileges. This model aims to prevent fraud, misuse, and resource theft. Assigning the Global Administrator role permanently to an individual contradicts this principle, as it allows one person to potentially deactivate security systems, wipe logs, disable backup safeguards, and release legal holds, particularly when there is less oversight, such as when the head of IT is away**. [Ex. 22A-7; Ex. 6G; Ex.24C-2]**

Fact 512: The overview of Requirement 7 emphasizes that access control measures must be applied universally, including to individuals like Ryan Brooks, Glenn Norris, Victor Brick, Justin Drummond, HEA, and others. As said in **Exhibit 22A-7 at 1**, "Unauthorized individuals may gain access to critical data or systems due to ineffective access control rules and definitions." It underscores that access rights should be governed by the principles of "need to know" and "least privileges." "Need to know" restricts access to the minimum necessary data for job performance, while "least privileges" grants only the minimum level of access needed. These principles are essential for securing user accounts and access for all personnel, including employees, contractors, and external vendors. **[Ex 12F-3 at 1]**

Fact 513: Emails sent by the Defendant, Ryan Dillon-Capps, between 1:16 PM on May 21, 2024, and 2:12 AM on May 22, 2024, demonstrate Dillon-Capps's good faith efforts, in contrast to Glenn Norris's obstruction to satisfy. The review of Dillon-Capps's emails should not be limited to this single day; the court is encouraged to request for examination the contents of May 20, 2024, to June 13, 2024, as the contents of the mailbox from the Defendant and others provides insights into the larger context for the hostile workplace, retaliation, whistleblower, and other legal issues that the Plaintiff is trying to avoid through their abusive use of the judicial system in this lawsuit. Norris's refusal to give any answer about Ryah Brooks work prevents satisfaction of PCI DSS requirement 7. **[Ex. 19A; Ex. 19B; Ex. 19C; Ex. 19D; Ex. 19E; Ex. 19F; Ex. 19G; Ex. 19H; Ex. 19I; Ex. 19J; Ex. 19K; Ex. 19L; Ex. 19M; Ex. 19N-1; Ex. 19N-2; Ex. 19O; Ex. 19P-1; Ex. 19P-2; Ex 12F-3 at 1]**

Fact 514: Richard Hartman, Justin Drummond, Glenn Norris, and Victor Brick are not responsible for maintaining PCI compliance and, therefore, do not have direct access that can negatively impact the cardholder data environment (CDE). They can only request access from Authorized Personnel, and this is what they have done for years. This is the first time they have refused to provide any information to satisfy requirement 7 and it makes their later demands unlawful with their threats an attempt to coerce the Defendant to violate their duty, the FDD contracts, and applicable laws that would apply from the act as well as from any event that occurred after that was linked back to that decision. PCI DSS v4 is mandated for the protection of private data which has a long-standing track record of being obtained because someone provided access in a manner that did not conform to these standards. Furthermore, Ryan

Brooks was sharing an account he had given Elevated Global Administrator rights to with multiple people that work at Baltimore Consulting, Victor Brick requires his assistant to remember his passwords, and Glenn Norris and Victor Brick poor security choices place them in the category of high-risk targets for having their bank, investment, and other financial sources compromised – again. These are not individuals demonstrating good decision making when it comes to the digital security of themselves, and the Defense cautions against a decision to believe that they understand the implications of their choices which is not in the publics best interest. **[Federal Trade Commission v. Wyndham Worldwide Corporation, et al., No. 2:13-cv-01887-ES-JAD (D.N.J. 2013); In the Matter of: BJ's Wholesale Club, Inc., FTC File No. 042 3160 (2005)]**

Fact 515: Ryan Brooks's refusal to participate in code review, change control, and daily stand-ups, while making changes outside of the proper approval process, violates PCI DSS Requirements 6 and 10. Requirement 6 focuses on developing and maintaining secure systems and applications, including implementing proper change management processes. Requirement 10 emphasizes tracking and monitoring access to network resources and cardholder data, including the need for logging and review procedures to maintain data security and integrity. **[Ex. 22A-6; Ex. 22A-10; Ex. 19G; 24C-2]**

Fact 516: Post-termination of Ryan Brooks and Baltimore Consulting, Dillon-Capps discovered adverse changes attributed to Brooks in the security systems, logs, backup safeguards, and legal holds. These actions potentially violate PCI DSS Requirements 6, which mandates secure maintenance and updates of systems, and Requirement 10, which emphasizes

maintaining the integrity of logs and security monitoring. The changes made without proper authorization or oversight could compromise the security and compliance of the cardholder data environment (CDE). **[Ex. 22A-6; Ex. 22A-10; Ex. 24C-2; Ex. 24E-2]**

Fact 517: Granting Ryan Brooks access again would violate multiple PCI DSS requirements. Specifically, Requirements 6 and 10 mandate secure system maintenance and monitoring, which Brooks previously compromised. Additionally, Requirement 8 emphasizes strong access control measures, including strict criteria for granting access to sensitive data and systems. Reintroducing Brooks, who has a documented history of non-compliance and unauthorized modifications, would not align with these standards, potentially exposing the organization to regulatory breaches and significant security risks. **[Ex22A-6; Ex.22A-8; Ex.22A-10]**

C Criminal Misuse of Executive Access

Fact 518: United States v. Scrushy, 721 F.3d 1288 (11th Cir. 2013) highlights the importance of segregation of duties and stringent access controls, as former HealthSouth CEO Richard Scrushy was implicated in a massive accounting fraud. The case underscores the dangers of failing to enforce proper controls over executive access, leading to significant financial abuse.

Fact 519: United States v. Kozlowski, 505 F.3d 120 (2d Cir. 2007) exemplifies how unchecked executive access can lead to large-scale embezzlement. Tyco International's CEO, Dennis Kozlowski, misused his access to authorize improper payments, demonstrating the need for strong oversight and access restrictions for high-level positions.

Fact 520: United States v. Madoff, 626 F.3d 34 (2d Cir. 2010) illustrates the risks of excessive executive access, as Bernie Madoff's control over investment records enabled him to perpetrate the largest Ponzi scheme in history. This case underscores the critical importance of implementing stringent access controls, especially for high-level executives, to prevent significant financial fraud.

Fact 521: These cases highlight the importance of Segregation of Duties (SoD) and enforcing least privileged access to prevent executives and other high-ranking individuals from abusing their positions to gain unnecessary access, which has a long-standing history of being linked to fraud. Without these controls, the risk of unethical actions by those in power will remain a significant threat to public trust and safety.

D Glenn Norris, Coercive Threats, and a Hostile Work Environment

Fact 522: Glenn Norris' refusal to provide information about what Ryan Brooks was being tasked to do conflicts with Requirement 7 of PCI DSS v4, which mandates the least privileged access. Refusing to provide necessary information while demanding access to be granted without information will result in Dillon-Capps violating PCI Compliance and subsequently breaching the FDD and MSA. Therefore, this is an unlawful order.

Fact 523: Refusal requires the ability to take action and asking for more information was the response, and then Norris did not reciprocate with a response.

Fact 524: Norris did not provide any response to the question. Norris then took a separate action in the form of a demand and coercive threat.

Fact 525: It is neither acceptable nor reasonable for an employer to threaten an employee who is lawfully performing their duties—duties that are in the public interest and mandated by industry standards, contractual obligations, and law.

Fact 526: Threatening an employee with employment consequences for refusing to follow an order that would violate PCI Compliance obligations constitutes a coercive act. Such threats contribute to creating a hostile work environment.

Fact 527: Filing a lawsuit without a factual basis to compel compliance with an unlawful order constitutes grounds for counterclaims of malicious prosecution and abuse of process.

E Reasonable Security and Least Privileged Access

Fact 528: Least privileged access is the technical term for the subject matter of Plaintiff's Complaint Exhibit 3, House Bill 925 from 1998, and the predecessor of **MD. Code Ann., Criminal Law §7-302(c)**. Also known as the legal basis for the Plaintiff's Complaint Count 3.

Fact 529: In 1998, the predecessor to **MD. Code Ann., Criminal Law §7-302(c)** was amended to include individuals who had authorized access but misused that access for unintended purposes. The principle of Least Privileged Access is the modern solution, standing for a company's due diligence to ensure that access provided does not exceed what is necessary for an individual to perform their job.

Fact 530: Similarly, we see in **United States v. Morris, 928 F.2d 504 (2d Cir. 1991)** early enforcement of the Computer Fraud and Abuse Act (CFAA), imposing severe penalties

for exploiting system vulnerabilities, even if the perpetrator had authorized access. In the 1990s and early 2000s, IT Departments were viewed as a cost to be managed by the finance department; exploiting system vulnerabilities were unstoppable and only limited by the hacker's capabilities, and the laws and enforcement reflected a post-compromised restoration.

Fact 531: In **Federal Trade Commission v. LifeLock, Inc., No. 2:10-cv-00530-MHM (D. Ariz. Mar. 9, 2010),** LifeLock was charged with failing to secure sensitive customer data, and in 2010, managing least privileged access effectively was a significant challenge. The costly settlement mandated enhanced security practices, including the implementation of a *zero-trust* architecture, which enforces strict access controls and incorporates the principle of least privileged access. The Tech Boom provided investment into technology leadership for CTOs and CIOs, but CFOs still viewed cybersecurity as an expensive overhead until cases like this created C-level security and shifted the conversation from secure to trust.

Fact 532: Least privileged access is a fundamental principle of modern cybersecurity frameworks, including the NIST Cybersecurity Framework and ISO/IEC 27001. Granting access beyond what is minimally necessary for a job role is considered negligent, especially for companies that have the technical capability to enforce the principle of least privileged access. In **United States v. Nosal, 676 F.3d 854 (9th Cir. 2012) (en banc)**, the Ninth Circuit ruled that the company's failure to implement least privileged access meant that an employee's misuse of company computers did not constitute a sufficient basis for charging the employee under the CFAA. This case highlighted the shift away from relying solely on judicial enforcement and

underscored the importance of businesses implementing "reasonable security" measures like those mandated by PCI DSS, which emphasizes least privileged access.

Fact 533: In **Federal Trade Commission v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015),** The Third Circuit upheld the FTC's authority to regulate corporate cybersecurity practices under the FTC Act, firmly establishing the FTC's role in enforcing standards like PCI Compliance. This case underscores the critical importance of incorporating least privileged access in cybersecurity frameworks to ensure that only authorized users can access sensitive data, thereby reducing the risk of breaches.

Fact 534: The timeline of these cases shows how the landscape of enforcement has changed since 1991 and that companies can no longer rely on federal, state, and local statutes as a mechanism of recovery or defense when they are negligent in their performance of due diligence, and they will be held liable for failure to secure their environment sufficiently through the implementation of least privileged access.

Fact 535: The necessity of robust access control management is further evidenced by the fact that every major data breach in the last 14 years has involved insufficient management of access controls, underscoring the critical need for businesses to adopt these security practices.

F Conclusion of PCI Compliance

46 PCI DSS is not merely a contractual obligation—it is the de facto law within the payment card industry, supported by widespread adoption, enforcement by major payment networks, consistent recognition by courts as a critical standard of care, and seamless alignment with

federal laws such as the GLBA, CFAA, FTC Act, and SOX, as well as state and local statutes like Maryland's PIPA, Tennessee's Identity Theft Deterrence Act, Florida's FIPA, California's CCPA, Washington's WPA, and the District of Columbia's Consumer Protection Procedures Act.

47 PCI DSS Compliance is codified into Nevada state law; other states are codifying compliance with security standards like PCI Compliance as a defense, and state and federal enforcement of laws have used compliance with PCI DSS as the defining standard for "reasonable security." Enforcement of PCI DSS Requirements and Incidents are codified in every state and multiple federal regulations.

48 Non-compliance with PCI DSS is not just a breach of industry expectations; it is a direct violation of these legal obligations. The statutes enforce what PCI DSS requires—protection against unauthorized access, secure systems, data encryption, robust authentication, and comprehensive security policies—making adherence to PCI DSS essential for both legal and operational compliance.

49 Intentionally violating PCI DSS is an intention to violate federal, state, and local laws, reflecting a conscious disregard for the legal and regulatory standards that safeguard consumers and the integrity of the financial system.

DECLARATION OF AFFIRMATION

I SOLEMNLY DECLARE AND AFFIRM UNDER PENAL TIES OF PERJURY AND UPON PERSONAL KNOWLEDGE THAT THE CONTENTS OF THE FOREGOING PAPER AND EXHIBITS THERETO ARE TRUE.

September 25, 2024

/s/ Ryan Dillon-Capps
Ryan Dillon-Capps (Pro Se)
Email: ryan@mxt3.com
1334 Maple Avenue
Essex, Maryland 21221
Telephone: (703) 303-1113

RESPECTFULLY SUBMITTED

September 25, 2024

/s/ Ryan Dillon-Capps
Ryan Dillon-Capps (Pro Se)
Email: ryan@mxt3.com
1334 Maple Avenue
Essex, Maryland 21221
Telephone: (703) 303-1113

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on September 25, 2024, a copy of **Affidavit OF LEGAL Obligations** via email to rbrennen@milesstockbridge.com and served on via first-class mail, postage prepaid on:

Robert S. Brennen
Miles & Stockbridge P.C.
100 Light Street
Baltimore, Maryland 21202

/s/Ryan Dillon-Capps
Ryan Dillon-Capps (Pro Se)