Are you compliant?

PCI Security Standards Council

U.S. Federal Trade Commission (FTC)

U.S. Department of Commerce

U.S. Department of Health & Human Services (HHS)

U.S. Department of Justice (DOJ)

Security and Privacy Compliance Scorecard

Does your business comply with federal, state and industry information security regulations? How much at risk are you right now?

Find out now with this fast and simple compliance scorecard.

Instructions: *Answer the questions below and add up the points for each "Yes" to see how you're doing right now in meeting the requirements of the laws, and in protecting your customers and your business against identity theft and fraud.*

Yes No

10 pts □ □ **1.** Were you **already aware** that your business must comply with specific federal, state and industry laws to protect your customers and employees against identity theft and fraud?

10 pts □ □ **2.** If your business accepts credit cards, are you already **PCI Compliant**?

Administrative / Physical Safeguards

10 pts □ □ **3.** Do you have a formal **Information Security Policy** for your business? If so, have you done a complete review and update of your policy guidebook in the last 12 months? *(Including Technical, Administrative, and Physical security and/or privacy policies and guidelines)*

10 pts □ □ **4.** Do you have a dedicated **Information Security Administrator** that is trained and responsible for managing your information security policies and procedures?

10 pts □ □ **5.** Do you have a "Red Flags" **identity theft detection**/ response program? *(Including on-going staff training & reporting procedures)*

10 pts □ □ **6.** Do you have an **employee/staff training program** for information privacy and security? *(And has everyone in your business completed this training?)*

20 pts □ □ **7.** Do you have formal employee **hiring and firing policies** and procedures to safeguard your business against insider security threats?

10 pts □ □ **8.** Have all your **employees signed** an Information Security and Privacy Agreement protecting you from insider theft and abuse?

10 pts □ □ **9.** Do you have a detailed **security breach response plan**? *(Including reporting to proper authorities and required communications to affected customers)*

20 pts □ □ **10.** Do you **securely dispose** of customer and employee information? *(Including secure computer data disposal, document shredding, etc.)*

10 pts □ □ **11.** Do you restrict **physical and electronic access** to customer and employee information? *(Including passwords, user authentication, locked filing systems, keyed entry, etc.)*

Technical Safeguards

Yes No

20 pts □ □ **12.** Have you installed a **hardware firewall** to protect your Internet connection, and properly configured it by closing unnecessary and high risk data ports?

10 pts □ □ **13.** If you have a **computer network** (of any size), do you have security software installed on your server(s)? *(And updated daily)*

10 pts □ □ **14.** Is **security software** installed and updated on every computer that connects to your business or your computer network? *(Anti-malware, desktop firewall, etc.)*

10 pts □ □ **15.** Have you changed the **manufacturers default passwords** on all your computers, servers, routers, wi-fi connections, etc.?

10 pts □ □ **16.** Do you **change passwords** regularly for all employee and system logins?

10 pts □ □ **17.** Do you have a computer security professional perform a **manual security checkup** on every computer and/or server regularly – at least quarterly or semi-annually? *(To ensure there are no hidden viruses, keyloggers, rootkits, etc. that may be stealing info.)*

20 pts □ □ **18.** Do you regularly check for and install all high priority **system patches** on each computer and server? *(To close security holes found and used by hackers to break in and steal information)*

10 pts □ □ **19.** Do you **encrypt** electronic copies of customer and employee information?

20 pts □ □ **20.** Do you conduct **vulnerability assessments** for your business on a quarterly or semi-annual basis? *(Including all Internet connections, network penetration testing, website scans, and computer vulnerability testing)*

Your Total Score □

0-100 points — **HIGH RISK**

110-150 points — **MEDIUM RISK**

Over **150** points — **LOW RISK**

Fines/Penalties for Non-Compliance:

Businesses who do not meet minimum standards for information security face **steep fines** and **penalties.**

- ➢ **Federal fines up to $3,500** per customer record stolen or lost. Owners, officers personally liable up to **$10,000** per violation.
- ➢ **State fines up to $5,000** per customer record stolen or lost. *(depending on each state)*
- ➢ **Credit card company penalties up to $10,000** on first violation for not implementing required safeguards.
- ➢ **Civil penalties up to $500,000** for failure to safeguard, keep private, properly dispose of personal or financial customer information.
- ➢ **Criminal penalties** including **jail time** for reckless or negligent disclosure of personal information.