Data Breach Incident Response Plan for IRONFRAME Media, LLC

Effective Date: October 21, 2025

At IRONFRAME Media, LLC ("we," "us," or "our"), a Texas-based real estate photography business located at 18425 Wolf Run, Needville, Texas 77461, we are committed to safeguarding client information and maintaining trust in our services. This Data Breach Incident Response Plan (IRP) outlines the procedures for identifying, responding to, containing, recovering from, and learning from a data breach or security incident. It aligns with our Information Security Policy, Privacy Policy, and Refund Policy, and ensures compliance with PCI DSS Requirement 12.10 (for payment processing via Intuit QuickBooks Merchant Services), the Texas Data Breach Notification Law (Tex. Bus. & Com. Code § 521.053), and other applicable regulations.

This IRP applies to all employees, contractors, and third-party vendors handling data for our operations in Southeast Texas. By participating in our services or accessing our systems (e.g., ironframemedia.com hosted by GoDaddy), you acknowledge this plan's role in protecting sensitive information, such as client personal data, payment details, and service-related records (e.g., property addresses, shoot details).

Our goal is to minimize damage, ensure timely notifications, and restore operations swiftly while preserving evidence for investigations.

1. Purpose

This IRP provides a structured roadmap to:

- Detect and classify potential breaches (e.g., unauthorized access to client emails, payment confirmations, or MS Office email lists).
- Contain and eradicate threats to prevent further harm.
- Recover systems and data securely.
- Notify affected parties (e.g., clients, Intuit, Texas authorities) within required timelines (e.g., 60 days under Texas law for breaches affecting 250+ residents).
- Conduct post-incident reviews to improve resilience, including PCI DSS self-assessments.
- Comply with PCI DSS by maintaining an incident response plan that is disseminated to personnel and reviewed annually.

2. Scope

This plan covers:

Data Types: Personal information (names, emails, phone numbers, addresses), payment data (transaction confirmations via QuickBooks; no full card details stored), service data (property details, shoot preferences, photos delivered digitally), and marketing data (realtor email lists compiled in MS Office from public sources).

Systems: ironframemedia.com (GoDaddy-hosted with analytics), QuickBooks Merchant Services links, MS Office tools, devices for photo editing/delivery, and email communications (e.g., for bookings or refunds).

Incidents: Any suspected or confirmed breach, including unauthorized access, data leaks, ransomware, phishing, or anomalies (e.g., unusual login to QuickBooks or GoDaddy dashboard).

Personnel: All involved parties, including sole member, Phillip Steffek, as primary responder, external vendors (e.g., Intuit, GoDaddy), and clients.

Exclusions: Minor IT issues (e.g., password resets) not involving data compromise.

3. Roles and Responsibilities

Clear roles ensure swift action. As a small business, Phillip Steffek serves as the primary Incident Response Coordinator, but we may engage external experts.

Role	Responsibilities	Contact
Incident Response Coordinator (IRC) (Phillip Steffek, Founder)	Lead detection, containment, notification, and recovery; coordinate with authorities.	979-349-1744 phillip@ironframemedia.com (mailto:phillip@ironframemedia.com)
Technical Responder (Phillip Steffek or IT contractor)	Isolate systems, analyze logs (e.g., GoDaddy analytics, QuickBooks audits), eradicate threats.	Designated contractor (if any); otherwise, IRC.
Legal/Compliance Advisor (External	Advise on notifications, contracts (e.g., Intuit	Retained Texas attorney.

Attorney to be retained in event of a data breach)	agreement), and Texas/PCI DSS compliance.	
Communications Lead (IRC)	Notify clients, vendors (e.g., Intuit), and authorities; manage PR (e.g., website updates).	phillip@ironframemedia.com (mailto:phillip@ironframemedia.com)
Third-Party Vendors (Intuit, GoDaddy)	Report breaches in their systems; assist with forensics (PCI DSS compliant).	Intuit: 1-800-446-8848 GoDaddy: 480-463-8824

All personnel must report suspicions immediately to the IRC and complete annual training on this IRP.

4. Incident Identification and Detection

We monitor for breaches using:

Tools: GoDaddy security alerts, QuickBooks transaction logs, MS Office access controls, and anomaly detection (e.g., unusual IP logins).

Triggers: Unauthorized access attempts, data export anomalies, client complaints (e.g., via 979-349-1744), or alerts from PCI DSS self-assessments.

Classification:

Low: Isolated event (e.g., phishing email); monitor only.

Medium: Potential compromise (e.g., suspicious login); investigate within 24 hours.

High: Confirmed breach (e.g., leaked client data); activate full IRP within 1 hour.

Upon detection, the IRC logs the incident (date, time, description) and assesses scope (e.g., affected clients in Harris County).

5. Containment

Immediate steps to limit damage:

    - Short-Term (0-24 hours): Isolate affected systems (e.g., disable QuickBooks links, change passwords on GoDaddy/MS Office). Preserve evidence (e.g., screenshots, logs without altering them).
    - Long-Term (24-72 hours): Deploy backups (encrypted, offsite) and engage forensics (e.g., Intuit's PCI-compliant tools).
    - Weather/Operational Tie-In: If a breach coincides with a shoot (e.g., compromised drone data), halt operations and reschedule per Refund Policy (no charge for weather/security issues).

6. Eradication

    - Remove threats: Scan systems with antivirus (e.g., Malwarebytes), patch vulnerabilities (e.g., GoDaddy updates), and delete unauthorized access.
    - For PCI DSS: Ensure no cardholder data remnants; consult Intuit for joint eradication.

7. Recovery

    - Restore operations: Test systems (e.g., 24-hour photo delivery workflow) before resuming.
    - Monitor for reoccurrence: 30-day post-recovery surveillance.
    - Resume services: Notify clients of safe resumption (e.g., via email with opt-out per Privacy Policy).

8. Notification Procedures

    - Timely, compliant notifications:
        - Internal: Alert team/contractors within 1 hour.
        - Affected Clients: Within 60 days (Texas law); provide details (what, when, how to protect) via email/phone (979-349-1744). Offer free credit monitoring if PCI data affected.
        - Vendors: Intuit (immediate for payment breaches); GoDaddy (per their terms).
        - Authorities:
            - Texas Attorney General (if 250+ residents affected): Within 30 days.
            - Card brands (via Intuit) for PCI incidents.

Public: If material risk, post on ironframemedia.com; no broad disclosure without legal advice.

9. Post-Incident Review

After-Action Report: Within 30 days, document lessons (e.g., update MS Office security for email lists).

Updates: Revise IRP annually or post-incident; train staff.

Metrics: Track response time, costs, and improvements (e.g., PCI DSS Requirement 12.10 compliance).

10. Testing and Maintenance

Annual tabletop exercises (simulate a QuickBooks breach).

Review with Intuit/GoDaddy annually.

Updates posted on ironframemedia.com and shared via email.

11. Contact Us

For incidents or questions:
Email: phillip@ironframemedia.com (Subject: "Security Incident Report")
Phone: 979-349-1744 (24/7 availability)
Address: 18425 Wolf Run, Needville, Texas 77461
For PCI-related breaches, contact Intuit at 1-800-446-8848.