



Should a Small Business Keep Collecting Social Security Numbers? A Case Report

October 03, 2026

Table of Contents

Executive Summary

Problem Statement and Engagement Scope

Decision problem

In scope

Out of scope

Success criteria

Methodology and Approach

Current-State Analysis

Baseline

Current-state evidence gaps

Implications

Key Findings

Options Considered

Option 1: Continue current collection and retention practices

Option 2: Continue broad collection with stronger protections

Option 3: Stop all collection and dispose of all existing holdings

Option 4: Collect only for verified requirements and dispose of other holdings

Recommendation

Reversal conditions

Pre-mortem

Risks, Assumptions, and Dependencies

Risks

Assumptions

Dependencies

Implementation Roadmap

Phase 1: Immediate containment and accountability

Phase 2: Inventory and purpose mapping

Phase 3: Requirement validation and policy approval

Phase 4: Controlled disposition and protection

Phase 5: Operating discipline and review

Next Steps

Disclaimers and Limitations

Sources

Should a Small Business Keep Collecting Social Security Numbers? A Case Report

Executive Summary

The owner should adopt a requirement based approach: stop collecting customer Social Security numbers unless a specific lawful or necessary business purpose has been documented, retain approved exceptions only for the necessary period, and securely dispose of all other holdings after retention requirements are confirmed.

RECOMMENDATION

Adopt a documented, requirement based collection rule. Retain customer Social Security numbers only when a specific lawful or necessary purpose is verified. Dispose of all other records securely after confirming retention obligations. Confidence: medium. The decision is partially reversible because approved records remain available, but destroyed records cannot be restored.

[Fact] Social Security numbers are sensitive personally identifying information. The Federal Trade Commission states that thieves commonly use such information to commit fraud or identity theft. [1]

[Fact] The Federal Trade Commission directs businesses not to collect or retain sensitive information without a legitimate business need. It also directs businesses to retain needed information only as long as necessary. [1]

[Inference] Broad customer collection cannot be supported by convenience, historical practice, permanent customer files, or use as a customer identifier. The available evidence supports collection only where a specific purpose is established.

[Assumption] The business is a small business that currently collects Social Security numbers from some customers. It retains those numbers in paper files and on computers. The business has no dedicated security staff and must decide within the next month.

[Inference] The recommendation balances two competing objectives. It reduces avoidable exposure from a highly sensitive identifier while preserving the ability to meet verified legal or operational obligations.

[Inference] This approach has a lower ongoing protection burden than continuing broad collection. It requires an initial inventory, purpose review, retention decision, and disposal effort. It does not remove the need to protect Social Security numbers that remain justified.

[Inference] The status quo has the highest apparent cost of inaction. It continues collection and retention while the business has not established why each customer number is needed, where all copies reside, or whether appropriate safeguards operate.

[Inference] An immediate universal disposal decision would reduce exposure more rapidly. However, it would create a material risk if a customer number is required for an unidentified legal, contractual, tax, credit, payment, or verification obligation.

[Inference] The recommended decision is partially irreversible. Ending unnecessary future collection is reversible if a valid purpose later emerges. Securely destroying existing records is not reversible. The owner should therefore validate retention obligations before authorizing disposal.

[Inference] Confidence is medium. The governing data minimization principles are explicit. Confidence is limited because the business has not provided the collection purposes, applicable obligations, record inventory, control environment, or incident history.

[Inference] No expected value estimate is possible. The source materials provide no record count, incident probability, loss estimate, implementation cost, or savings estimate. The qualitative expected value case favors reducing avoidable retained inventory because retained information can be exposed, while unheld information cannot be stolen from the business system. [1]

[Inference] The next step is a bounded fact finding exercise led by the owner. It should identify every collection purpose, validate each retention requirement, locate every copy, stop clearly unjustified new collection, and preserve uncertain records until final classification.

Problem Statement and Engagement Scope

The decision is whether the business should keep collecting Social Security numbers from customers or stop. The owner must select a practical approach within the next month.

DECISION PROBLEM

[Fact] Sensitive data that falls into the wrong hands can lead to fraud, identity theft, or similar harms. A security breach can also result in lost customer trust and potential legal defense costs. [1]

[Inference] The central question is not whether Social Security numbers have value in every circumstance. The question is whether each requested customer number has a verified purpose that justifies collection, retention, and protection.

[Assumption] The business has limited time and budget. It lacks dedicated security specialists. These conditions make a broad, control intensive collection model less practical than a limited, purpose based model.

IN SCOPE

- Customer Social Security number collection, storage, access, retention, protection, and disposal.
- Paper files, computers, laptops, portable devices, email, backups, home working locations, digital copiers, and service providers that may contain customer records.
- Controls appropriate for retained customer Social Security numbers.
- A decision path that can be initiated within the next month.

OUT OF SCOPE

- Legal advice or a determination of specific legal duties.
- Design of a complete enterprise security program beyond controls relevant to retained customer Social Security numbers.
- Assessment of employee Social Security numbers, except where systems or controls overlap with customer data.
- Quantification of breach losses, implementation costs, savings, or operational impacts.

SUCCESS CRITERIA

[Assumption] The decision should reduce potential harm from loss or theft, preserve the ability to operate and meet verified obligations, and remain feasible for a small team without security specialists.

[Inference] A successful outcome will establish a written collection rule, a record inventory, documented retention decisions, proportionate safeguards for exceptions, secure disposal procedures, and accountable ownership.

Methodology and Approach

This assessment uses the supplied Federal Trade Commission guidance as the sole factual basis. It distinguishes source supported facts from conclusions and case conditions that have not been independently verified.

[Fact] The Federal Trade Commission presents five key principles for a sound data security plan: take stock, scale down, lock it, pitch it, and plan ahead. [1]

The analysis applies those principles in sequence. First, it considers what information may exist and where it may reside. Second, it tests whether collection and retention have a legitimate business purpose. Third, it considers proportionate protections for records that remain. Fourth, it addresses secure disposal. Fifth, it considers readiness for a security incident.

[Fact] The Federal Trade Commission advises businesses to identify the personal information they hold, where it is stored, how it moves through the business, and who has or could have access to it. [1]

Evidence confidence is treated conservatively. [Fact] claims are limited to statements supported by the supplied source and include citations. [Inference] claims derive from those facts and the stated

decision context. [Assumption] claims identify unverified conditions from the case description or information gaps.

[Inference] No probability estimates are presented because the source materials provide no base rates for compromise, fraud, identity theft, control failure, or breach costs. Qualitative likelihood assessments therefore indicate directional exposure, not statistical forecasts.

[Inference] No monetary expected value calculation is presented because the necessary inputs are unavailable. The report instead compares expected directional effects: exposure reduction, operational continuity, control burden, reversibility, and opportunity cost.

Current-State Analysis

BASELINE

[Assumption] The business collects Social Security numbers from at least some customers. It retains them in paper files and on computers.

[Fact] Many data compromises happen through lost or stolen paper documents. The Federal Trade Commission recommends storing paper records containing personally identifiable information in locked rooms or locked file cabinets. Access should be limited to employees with a legitimate business need. [1]

[Fact] The Federal Trade Commission recommends identifying the computers and servers where sensitive information is stored. It also recommends identifying all connections to those systems and assessing each connection for commonly known or reasonably foreseeable attacks. [1]

[Inference] The assumed storage in paper and electronic forms creates two principal exposure pathways. Paper records may be lost, stolen, viewed, or mishandled. Electronic records may be exposed through system connections, weak authentication, malware, unencrypted storage, unencrypted transmission, unauthorized access, or incomplete disposal.

CURRENT-STATE EVIDENCE GAPS

Area	Known position	Unverified condition	Decision implication
Collection purpose	[Assumption] Customer Social Security numbers are collected.	[Assumption] The purpose for each request is unknown.	[Inference] The business cannot establish whether broad collection is justified.
Retention obligations	[Fact] Social Security numbers should be used only for required and lawful purposes. [1]	[Assumption] Applicable obligations are unknown.	[Inference] Disposal cannot proceed safely until retention requirements are validated.
Record locations	[Assumption] Paper files and computers contain records.	[Assumption] Copies in backups, email, portable devices, home locations, copiers, and provider systems are unknown.	[Inference] Disposal scope and residual exposure cannot be estimated.

Area	Known position	Unverified condition	Decision implication
Controls	[Fact] The source identifies physical, electronic, employee, and provider controls. [1]	[Assumption] Existing safeguards are unknown.	[Inference] Current protection adequacy cannot be assessed.
Access	[Fact] Access should follow least privilege. [1]	[Assumption] Employee and provider access is unknown.	[Inference] The business cannot confirm that access is limited to need to know roles.
Incident readiness	[Fact] The source recommends an incident response plan and a designated senior coordinator. [1]	[Assumption] A response plan and incident history are unknown.	[Inference] Readiness to contain a loss cannot be assessed.

IMPLICATIONS

[Fact] The Federal Trade Commission states that information not held in a system cannot be stolen from that system by hackers. [1]

[Inference] The business can reduce exposure by reducing the volume and duration of retained customer Social Security numbers. This reduction is complementary to, rather than a substitute for, safeguards over justified records.

[Fact] The Federal Trade Commission states that a data security approach should fit the nature of the business and the information collected. It does not prescribe a one size fits all approach. [1]

[Inference] A small business without dedicated security staff should not assume that more controls alone solve the decision. Broad retention creates continuous administrative obligations, including access management, patching, training, inventory maintenance, disposal, vendor oversight, and incident readiness.

Key Findings

- [Fact] Social Security numbers are sensitive personally identifying information. The source states that thieves commonly use Social Security numbers, credit card information, financial information, and other sensitive data to commit fraud or identity theft. [1]
- [Fact] The source directs businesses not to collect or retain sensitive personally identifying information when there is no legitimate business need. It directs businesses to retain needed information only as long as necessary. [1]
- [Inference] Continuing broad customer collection without documented purpose validation is inconsistent with the source's data minimization direction. The present record does not establish that every collected customer number is needed.

- [Inference] Stronger controls can reduce unauthorized access risk for retained records. They cannot remove the inherent exposure created by retaining an unnecessary sensitive identifier.
- [Inference] A documented, requirement based collection rule offers the most balanced path. It preserves verified needs while reducing unnecessary collection, retention, and associated control burden.

Options Considered

The options are assessed against exposure reduction, operational continuity, feasibility, reversibility, and opportunity cost. No option is quantified because the materials do not provide costs, record volumes, breach probabilities, or control effectiveness data.

Option	Exposure reduction	Operational continuity	Feasibility for small team	Reversibility	Opportunity cost
Continue current collection and retention practices	[Inference] Weak. Broad retained exposure continues.	[Inference] Strong in the immediate term.	[Inference] Easy initially, but unresolved protection work remains.	[Inference] Reversible later, but delay can increase records requiring review.	[Inference] Defers process redesign, but consumes future management attention and retains avoidable exposure.
Continue broad collection with stronger protections	[Inference] Moderate. Controls may reduce likelihood or severity, but broad retention remains.	[Inference] Strong if broad collection is needed.	[Inference] Moderate to weak. Ongoing controls require sustained administration.	[Inference] Reversible, but control investment may precede need validation.	[Inference] Directs scarce time and funds toward protecting records that may not be necessary.
Stop all collection and dispose of all existing holdings	[Inference] Strong after verified disposal.	[Inference] Unknown until obligations are validated.	[Inference] Moderate. Inventory and secure disposal require disciplined execution.	[Inference] Least reversible after destruction.	[Inference] Reduces future protection effort, but may forgo necessary operational or compliance capability.
Collect only for verified requirements and dispose of other holdings	[Inference] Strong. Unnecessary collection and retention are reduced.	[Inference] Strong potential fit because verified needs remain supported.	[Inference] Moderate to strong. Initial classification effort reduces ongoing burden.	[Inference] Partially reversible. Required records remain, but destroyed records cannot be restored.	[Inference] Requires near term owner attention, but avoids sustaining broad controls over unjustified records.

OPTION 1: CONTINUE CURRENT COLLECTION AND RETENTION PRACTICES

[Assumption] This option retains current collection from some customers and stores Social Security numbers in paper files and on computers without a demonstrated change in collection rules or safeguards.

[Inference] The principal advantage is immediate continuity. The business would avoid redesigning forms, processes, retention rules, and disposal procedures in the short term.

[Fact] The source advises businesses not to collect or keep sensitive information without a legitimate business need. [1]

[Inference] The option has weak alignment with that direction because the present case does not establish a purpose for each customer number. It also creates a risk of normalizing collection because it is convenient or historic.

OPTION 2: CONTINUE BROAD COLLECTION WITH STRONGER PROTECTIONS

[Assumption] This option preserves broad collection while adding physical, electronic, access, training, disposal, provider management, and incident response controls.

[Fact] The source recommends inventorying data, restricting access, locking paper records, encrypting sensitive stored and transmitted information, using strong passwords, applying vendor approved patches, training employees, securely disposing of records, and planning for incidents. [1]

[Inference] This option may be appropriate if the business substantiates a need for most customer Social Security numbers. It is not a complete answer if broad collection lacks a legitimate purpose.

[Inference] The opportunity cost is significant in qualitative terms. Owner and staff attention would be allocated to protecting a broad inventory rather than reducing unnecessary inventory at its source.

OPTION 3: STOP ALL COLLECTION AND DISPOSE OF ALL EXISTING HOLDINGS

[Assumption] This option ends customer Social Security number collection and securely disposes of records already held.

[Fact] The source recommends shredding, burning, or pulverizing paper records before discarding them. It recommends wipe utility programs that overwrite hard drives when disposing of old computers and portable storage devices. [1]

[Inference] This option would materially reduce future collection and retained inventory. It creates a high decision risk if any records are needed for an unverified obligation.

[Inference] The owner should not select this option until legal and business retention requirements are confirmed. Secure destruction should follow a complete inventory and controlled execution.

OPTION 4: COLLECT ONLY FOR VERIFIED REQUIREMENTS AND DISPOSE OF OTHER HOLDINGS

[Assumption] This option requires the business to document valid customer specific collection purposes, collect only in those circumstances, set retention periods, and securely destroy other

records.

[Fact] The source recommends a written records retention policy that identifies what information must be kept, how it will be secured, how long it will be kept, and how it will be securely disposed of. [1]

[Inference] This option most directly applies the source's scale down principle. It reduces the population requiring protection while preserving records needed for verified purposes.

Recommendation

The owner should stop collecting customer Social Security numbers by default. The business should collect and retain them only where a specific lawful or necessary purpose is documented, with a defined retention period and proportionate safeguards.

RECOMMENDATION

Simple decision rule: Do not request, retain, or use a customer Social Security number unless the owner has approved a documented, specific lawful or necessary purpose. Preserve uncertain existing records until obligations are reviewed. Securely dispose of records outside approved purposes.

[Fact] The Federal Trade Commission states that Social Security numbers should be used only for required and lawful purposes. It specifically advises against using them unnecessarily as customer identification numbers or because of historical practice. [1]

[Inference] The recommendation accepts an initial implementation trade off. The business must spend management time on inventory, purpose validation, policy creation, staff communication, and disposal. This effort is preferable to continuing to administer broad protection obligations for records that may have no verified purpose.

[Inference] The recommendation rejects the status quo because current collection purposes and safeguards are unverified. It rejects protection of broad collection as the primary response because protection does not justify unnecessary collection. It does not recommend immediate universal destruction because requirements have not been validated.

[Inference] The decision is partially reversible. The business can add a narrowly defined collection purpose later if one is validated. However, records securely destroyed under an approved schedule cannot be recovered.

[Inference] Confidence is medium. The recommendation follows explicit source guidance on minimization and retention. It remains conditional on validation of applicable legal, contractual, operational, and retention requirements.

REVERSAL CONDITIONS

- [Assumption] A documented review establishes that a broader category of customer Social Security numbers is required for a specific lawful or necessary business function.
- [Assumption] A legal review identifies a retention obligation that requires a different collection or retention rule.
- [Assumption] The business identifies a customer process where a Social Security number is necessary and cannot reasonably be replaced by a less sensitive identifier.
- [Assumption] An inventory reveals an existing obligation or system dependency that requires a controlled transition before collection can cease.

PRE-MORTEM

[Inference] Assume the recommendation fails. The following failure modes require active prevention.

Potential failure	Early warning sign	Preventive action
[Inference] Necessary records are destroyed.	[Assumption] Staff identify an unresolved customer process or obligation after disposal approval.	[Inference] Require documented retention validation and owner approval before destruction.
[Inference] Copies remain after disposal.	[Assumption] Records are found in email, backups, portable devices, or provider systems.	[Inference] Complete an inventory across all storage locations before disposal certification.
[Inference] Staff continue requesting numbers out of habit.	[Assumption] Forms, scripts, or system fields still request the number without an approved purpose.	[Inference] Remove unnecessary fields and train staff on the approved decision rule.
[Inference] Retained exceptions remain weakly protected.	[Assumption] Access lists, locked storage, passwords, or encryption are incomplete.	[Inference] Apply least privilege, physical security, electronic protections, and periodic review.

Risks, Assumptions, and Dependencies

RISKS

Risk	Likelihood	Impact	Response direction
[Inference] Unauthorized access, theft, or loss of retained customer Social Security numbers.	[Inference] Medium. Paper and electronic storage are assumed, but controls are unknown.	[Inference] High. The source links exposure to fraud, identity theft, lost trust, and possible legal defense costs. [1]	[Inference] Reduce collection and retention. Lock paper records. Restrict access. Protect electronic environments.
[Inference] Necessary records are destroyed or collection stops before obligations are identified.	[Inference] Unknown. Applicable requirements are not provided.	[Inference] Potentially high.	[Inference] Validate requirements before authorizing destruction or final cessation.

Risk	Likelihood	Impact	Response direction
[Inference] Incomplete disposal leaves recoverable copies.	[Inference] Medium. The source identifies numerous storage locations for sensitive data. [1]	[Inference] High.	[Inference] Inventory paper, devices, backups, email, home locations, copiers, and service providers.
[Inference] Safeguard implementation fails because the small team lacks capacity.	[Inference] Medium to high.	[Inference] Medium to high.	[Fact] Some protections, including strong passwords, locked paperwork, and staff training, can cost next to nothing. [1]
[Inference] Staff incentives favor collecting more information for convenience, faster processing, or future optional use.	[Inference] Medium. Existing collection purpose is not documented.	[Inference] High if convenience overrides minimization.	[Inference] Require owner approved purposes and prohibit use of Social Security numbers as routine customer identifiers.
[Inference] The owner delays action because current collection appears operationally easy.	[Inference] High while needs, locations, access, and protections remain unverified.	[Inference] High because avoidable exposure continues.	[Inference] Set immediate inventory and validation milestones within the next month.

[Inference] The inversion view is material. The recommendation could produce harm if it causes premature destruction, overlooks a required process, leaves hidden copies, or creates staff workarounds. The roadmap addresses these failure modes through validation, inventory, controlled disposal, and approval gates.

ASSUMPTIONS

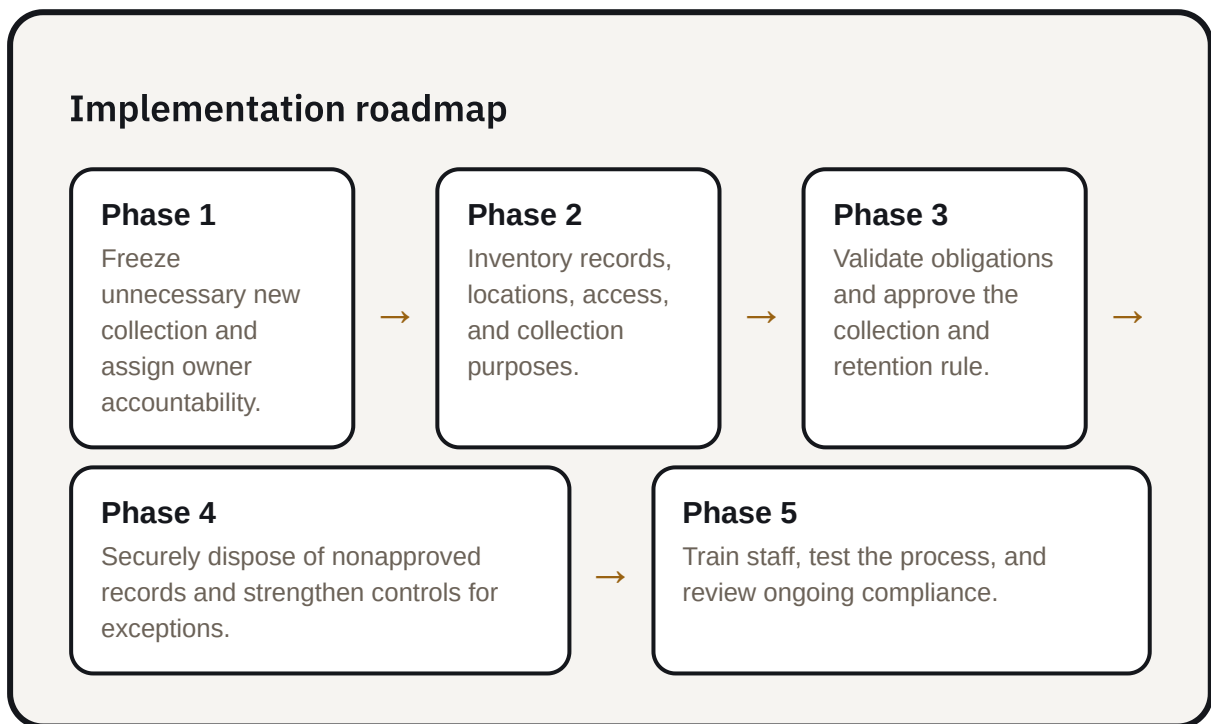
- [Assumption] The business is a small business and the owner is the decision maker.
- [Assumption] Customer Social Security numbers are held in paper files and on computers.
- [Assumption] The business lacks dedicated security staff and has limited time and budget.
- [Assumption] The business has not documented all collection purposes, retention requirements, records, access roles, controls, providers, or incident procedures.
- [Assumption] The decision must be made within the next month.

DEPENDENCIES

- [Inference] Owner sponsorship and final approval of collection and retention purposes.
- [Inference] Legal or qualified compliance review of applicable collection and retention requirements.
- [Inference] Cooperation from staff who manage customer intake, records, accounting, operations, and technology.
- [Inference] Identification of provider systems, storage locations, and access arrangements.

- [Inference] Availability of secure paper destruction and secure electronic wiping capabilities.
- [Inference] Completion of staff instructions and process changes before finalizing collection cessation.

Implementation Roadmap



[Inference] The roadmap is sequenced to prevent irreversible disposal before retention requirements are assessed. The owner should retain decision authority throughout.

PHASE 1: IMMEDIATE CONTAINMENT AND ACCOUNTABILITY

Owner: Business owner. Timing: immediately.

- [Inference] Direct staff not to request a customer Social Security number unless an existing, documented process requires it pending review.
- [Inference] Designate the owner as the senior coordinator for the decision and any related security incident.
- [Fact] The source recommends designating a senior staff member to coordinate and implement an incident response plan. [1]
- [Inference] Preserve existing records during the review. Do not destroy records until retention requirements are validated.

PHASE 2: INVENTORY AND PURPOSE MAPPING

Owner: Business owner, with records, operations, and technology support. Timing: during the next month.

- [Fact] The source recommends inventorying computers, laptops, mobile devices, flash drives, disks, home computers, digital copiers, and other equipment to locate sensitive data. [1]
- [Inference] Identify each customer process that requests a Social Security number, the stated purpose, the responsible employee, the receiving system, and each storage location.
- [Inference] Identify employees, contractors, and service providers with actual or potential access.
- [Fact] The source recommends tracking how personal information enters, moves through, and exits the business. [1]

PHASE 3: REQUIREMENT VALIDATION AND POLICY APPROVAL

Owner: Business owner, supported by qualified legal or compliance advice. Timing: before any disposal authorization.

- [Inference] Classify each collection purpose as approved, unapproved, or pending validation.
- [Inference] Create a written retention policy for approved purposes. Specify what must be retained, how it will be secured, retention duration, and disposal method.
- [Fact] The source recommends a written records retention policy with those elements. [1]
- [Inference] Establish a simple approval rule: no customer Social Security number may be collected without a documented approved purpose.

PHASE 4: CONTROLLED DISPOSITION AND PROTECTION

Owner: Business owner, with designated records and technology custodians. Timing: after Phase 3 approval.

- [Fact] The source recommends shredding, burning, or pulverizing paper records before discarding them. [1]
- [Fact] The source recommends wipe utility programs that overwrite hard drives when disposing of old computers and portable storage devices. [1]
- [Inference] Document disposal completion by location and record category. Include provider held and backup copies where applicable.
- [Fact] The source recommends locking retained paper records, encrypting sensitive stored and transmitted information, using strong passwords, and considering multi factor authentication. [1]
- [Inference] Apply least privilege access to all approved retained exceptions.

PHASE 5: OPERATING DISCIPLINE AND REVIEW

Owner: Business owner and supervisors. Timing: following implementation and on an ongoing basis.

- [Fact] The source recommends regular employee training, procedures for departing workers, and immediate reporting of potential security breaches. [1]

- [Inference] Train staff on the collection rule, approved uses, secure handling, escalation process, and prohibition on routine identifier use.
- [Inference] Review access rights, collection forms, scripts, retention schedules, and provider arrangements periodically.
- [Fact] The source recommends verifying service provider security practices, placing security expectations in contracts, and requiring incident notification. [1]

Next Steps

- 1. Owner, immediately:** Issue an interim instruction that staff must not initiate new customer Social Security number collection unless an existing documented process requires it.
- 2. Owner and records custodian, immediately:** Preserve all existing records while the retention review occurs. Do not authorize disposal based on assumptions.
- 3. Owner and functional leads, during the next month:** Complete an inventory of physical, electronic, backup, portable, remote, copier, email, and provider locations.
- 4. Owner with qualified legal or compliance support, during the next month:** Validate each claimed collection and retention requirement.
- 5. Owner, after validation:** Approve a written collection rule and retention policy. Classify records for retention or secure disposal.
- 6. Records and technology custodians, after approval:** Execute documented secure disposal for nonapproved records and apply protections to retained exceptions.
- 7. Owner and supervisors, after implementation:** Train staff, remove unapproved form fields and scripts, confirm access restrictions, and establish periodic review.

Disclaimers and Limitations

This report relies exclusively on the supplied Federal Trade Commission guidance for factual claims. It does not independently verify the business's collection practices, data locations, controls, contracts, legal duties, record volumes, incident history, or operational dependencies.

[Assumption] Statements about the business being small, retaining customer Social Security numbers in paper and electronic form, lacking dedicated security staff, and needing a decision within the next month are unverified case conditions.

This report is not legal advice. Determining whether a customer Social Security number must be collected or retained requires qualified review of applicable legal, contractual, tax, credit, payment, identity verification, and records retention obligations.

This report does not provide technical implementation assurance. The business should obtain competent assistance where it lacks the capability to assess systems, implement safeguards,

validate electronic disposal, or evaluate service providers.

[Fact] The Federal Trade Commission notes that statutes such as the Gramm Leach Bliley Act, the Fair Credit Reporting Act, and the Federal Trade Commission Act may require reasonable security for sensitive information. [1]

The analysis is valid only for the stated decision and the information supplied. Material changes in the business's obligations, data uses, systems, providers, or record locations may change the recommendation.

This report is intended for the owner and authorized decision makers. It should not be treated as a substitute for legal, compliance, security, or operational due diligence.

Sources

1. Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, October 2016.