72-Hour Breach Lockdown Checklist

Actionable steps after identity compromise — complete in order. Lock down access and identity first; broker opt-outs are medium-term surface reduction.

Outset Solutions LLC · EIN 92-1990340 · outset-solutions.com/checklist.html

If you have been compromised more than once, assume you are target-profiled. Complete Phases 1–3 before broker opt-outs. MFA is only as strong as your weakest recovery option — strip SMS and security-question backdoors before anything else.

Phase 1 — Stop active access (Day 1)

Primary email and phone number are the keys to every account. Lock the carrier and remove recovery backdoors before password changes stick.

1. Call mobile carrier — request SIM swap / port freeze and verbal PIN
2. Document carrier case number and representative name
3. Remove phone numbers from Google account recovery options
4. Remove phone numbers from Apple ID account recovery
5. Remove phone numbers from Microsoft account recovery
6. Remove phone numbers from banking and brokerage account recovery settings
7. Enable hardware security keys (YubiKey / FIDO2) on primary email account
8. Register passkeys on email and banking where supported — never use SMS 2FA on critical accounts
9. Enable authenticator app (TOTP) only where hardware keys or passkeys are unavailable
10. Register a secondary hardware security key as backup recovery; store keys in separate locations
11. Delete security questions; store one-time backup codes offline in a fire-safe location
12. Verify "Forgot password" cannot bypass hardware keys via SMS or security questions on critical accounts
13. Change password on primary email (new unique passphrase, 16+ chars)
14. Change password on online banking and brokerage accounts
15. Change password on IRS and SSA online accounts if enrolled
16. Revoke active OAuth sessions on Google, Apple, and Microsoft
17. Review recent sign-in activity on email and cloud accounts
18. Sign out of all devices on email and financial accounts
19. Disable call forwarding on mobile and VoIP lines
20. Check mail forwarding rules in webmail (attackers add hidden forwards)
21. Enable login alerts on financial institutions that support them
22. Freeze debit cards and request reissue if account takeover suspected

Phase 2 — Freeze financial identity (Day 1–2)

Public broker data makes new-account fraud easier. Freezes are free and take under 15 minutes total across all four bureaus.

23. Freeze Equifax — equifax.com/personal/credit-report-services/credit-freeze/
24. Freeze Experian — experian.com/freeze
25. Freeze TransUnion — transunion.com/credit-freeze

26. Freeze Innovis — innovis.com/personal/securityFreeze (often overlooked fourth bureau)
27. Save each bureau confirmation number and freeze PIN offline
28. Request IRS Identity Protection PIN (IP PIN) at irs.gov/ippin
29. Review ChexSystems consumer report if checking accounts were targeted
30. Review NCTUE (telecom/utility) report if phone or utility fraud occurred
31. Place fraud alert or verify existing freezes are active on all four bureaus
32. Notify primary bank fraud department with FTC report number when available
33. Review recent ACH, wire, and Zelle activity for unauthorized transfers
34. Document every financial institution contacted with date, rep, and case number

Phase 3 — Document and report (Day 2–3)

Skip reporting steps you have already completed — keep confirmation numbers in your evidence folder.

35. File identity theft report at IdentityTheft.gov (FTC) — skip if already filed; download confirmation PDF
36. Save FTC Identity Theft Report and confirmation number offline (skip if already on file)
37. File IC3 report at ic3.gov if financial theft or unauthorized access occurred
38. Contact local police for a report if your state requires it for credit disputes
39. Contact CFPB if consumer reporting or financial account errors are involved — skip if already filed
40. Notify SSA Office of Inspector General if SSN misuse is suspected
41. Request fraud alerts on investment and retirement accounts
42. Pull free credit reports from AnnualCreditReport.com (one bureau at a time)
43. Highlight unauthorized inquiries and accounts on credit reports
44. Save confirmation numbers, screenshots, and emails in an offline evidence folder
45. Create a chronological incident log (date, account, action, outcome)
46. Share FTC report number with banks when disputing fraudulent transactions
47. Set calendar reminders for 7-day and 30-day follow-ups on open disputes
48. Back up evidence folder to encrypted offline storage (not cloud-only)

Phase 4 — Upstream broker opt-outs (Week 1+)

Only after Phases 1–3. Do not waste time on minor downstream people-search sites first — target upstream aggregators that supply them.

49. LexisNexis — submit consumer suppression request
50. Acxiom — submit marketing data opt-out
51. LiveRamp — complete identity opt-out form
52. Verisk — opt out of marketing databases and data products
53. Epsilon — submit marketing data opt-out
54. Oracle Data Cloud (formerly Datalogix) — opt out where available
55. Experian Marketing Services — opt out of marketing data sales
56. TransUnion marketing opt-out (separate from credit freeze portal)
57. Equifax marketing opt-out (separate from credit freeze portal)
58. CoreLogic SafeRent — opt out if rental or tenant screening dossiers exist
59. Innovis consumer opt-out (in addition to credit freeze)
60. Review CFPB list of consumer reporting companies for your industry dossiers

61. Opt out of MIB (insurance history) if life or health insurance was targeted

62. Opt out of NCTUE telecom/utility data sharing if not done in Phase 2

63. Submit opt-out to major people-search sites (Spokeo, BeenVerified, Whitepages)

64. Queue batch opt-outs via Privacy Dawg or manual spreadsheet workflow

65. Screenshot each opt-out confirmation page with date stamp

66. Track broker response deadlines (typically 30–45 days)

67. Re-scan Google results for your name + city after 30 days

68. Dispute reappeared listings with proof of prior opt-out confirmation

69. Remove old addresses from USPS change-of-address if fraudulently filed

70. Request data broker lists from background-check vendors used by employers

71. Opt out of marketing lists at DMAchoice.org and NAI opt-out page

72. Schedule quarterly broker re-scan (Privacy Pro or manual process)

Phase 5 — Maintenance (ongoing)

73. Quarterly re-scan for reappeared broker listings and new exposures

74. Annual credit report review via AnnualCreditReport.com (rotate bureaus)

75. Re-freeze credit after any temporary thaw for legitimate applications

76. Rotate email and banking passwords annually or after any new breach notice

77. Verify hardware security keys and passkeys still registered on critical accounts

78. Review mobile carrier port-freeze status — renew if carrier requires it yearly

Print and check off each step. This checklist is educational — not legal advice. Not affiliated with the U.S. Department of Veterans Affairs.

Generated 2026-07-06 08:28 UTC · 78 steps · Outset Solutions LLC