ALPHATRUST ADVISORS

Information Security Incident Response Program Summary

AlphaTrust Advisors®

5141 N. 40th Street, Suite 400
Phoenix, Arizona 85018
alphatrustadvisors.com

VER. 2.0

About this Summary

This document summarizes the Information Security Incident Response Program (the "ISIRP") maintained by AlphaTrust Advisors. It is provided in response to client, counterparty, and request-for-proposal information requests. The full Program is an internal document; this summary describes the substantive controls and notification commitments without operational identifiers. AlphaTrust Advisors will discuss additional detail under an appropriate confidentiality arrangement.

1. Scope

"AlphaTrust Advisors" refers to AlphaTrust Advisory Group, LLC, AlphaTrust Law Group, LLC, AlphaTrust Tax Services, LLC, AlphaTrust Insurance Services, LLC, and any affiliated entity operating under the AlphaTrust brand. **The Program applies to all of those entities and to their employees.**

The Program is designed to meet the Firm's obligations under SEC Regulation S-P (as amended May 2024), the FTC Safeguards Rule, the Arizona breach notification statute (A.R.S. § 18-552), state insurance data security laws based on NAIC Model #668 (in adopting states where the Firm holds producer licenses), 23 NYCRR Part 500 (where applicable), and Arizona Rule of Professional Conduct ER 1.4 (interpreted per ABA Formal Opinion 483) and ER 1.6(e) for the Firm's legal practice.

2. Governance

A single Responsible Person (the Chief Compliance Officer) leads the Program and serves as incident commander, with a Backup Responsible Person (the President). The Firm engages a managed IT services provider for technical preservation and recovery, maintains cyber liability insurance with a 24/7 breach response hotline, and will engage breach counsel when required. All external notifications are authorized by the Responsible Person in coordination with counsel and with President approval.

3. Incident Classification

Routine events (e.g., a phishing email reported before any user interaction; spam caught by a filter) do not activate the Program. Incidents that require investigation are tiered:

Level	Examples	Initial Response	Update Cadence
Level 1 (Critical)	Confirmed or reasonably likely unauthorized access to Sensitive Customer Information; ransomware; active intrusion; account takeover with client-funds exposure; EFIN compromise; any event triggering a mandatory regulatory report.	Within 1 hour of detection	Every 1 to 4 hours until contained
Level 2 (Significant)	Suspicious activity requiring investigation; phishing where a user entered credentials but downstream access has not been confirmed; vendor-reported incident of unknown scope; lost or stolen unencrypted device.	Within 1 business day	Daily until contained
Level 3 (Low)	Internal policy violation contained without external exposure; longer-running investigation of suspicious activity where harm is unlikely.	Within 3 business days	Weekly until closed

Note: These internal response cadences are the Firm's operating standard. External notification deadlines are governed by Section 5.

4. Lifecycle

Every Incident proceeds through six phases, each logged in the Firm's Incident Log: identify and triage, contain, eradicate, recover, notify, and post-incident review. Post-incident review is conducted within 30 days of closure and includes timeline, root cause, control failures, and remediation actions with owners and deadlines.

5. External Notification Standards

The Firm meets the strictest applicable deadline for any given Incident. The principal external deadlines:

Recipient	Trigger	Outer Deadline
Affected individuals (federal floor)	Unauthorized access to or use of Sensitive Customer Information reasonably likely to result in substantial harm or inconvenience (Reg S-P).	As soon as practicable, no later than 30 days from determination
Affected Arizona residents	Unauthorized acquisition of unencrypted, unredacted Personal Information (A.R.S. § 18-552).	Within 45 days of determination
AZ Attorney General + AZ DHS + nationwide CRAs	Same trigger as above where more than 1,000 AZ residents must be notified (A.R.S. § 18-552(D)).	Within 45 days

Recipient	Trigger	Outer Deadline
FTC	Notification event involving unencrypted Customer Information of 500 or more consumers (16 CFR § 314.4(j)).	As soon as possible, no later than 30 days from discovery
State insurance commissioner (non-resident license states with Model #668-based laws)	Incident affects 250 or more residents of that state AND notice is required to any other governmental body (NAIC Model #668 § 6).	Within 72 hours of determination
NYDFS (if NY non-resident license held)	Incident that is a Cybersecurity Incident under 23 NYCRR § 500.1(g).	Within 72 hours of determination, via the DFS Portal
IRS (Tax practice)	Data theft involving taxpayer data; ID-theft pattern; EFIN compromise (IRS Pubs 4557, 5708, 5293, 1345).	As soon as possible; within 1 business day for an Authorized e-file Provider security incident
Affected legal clients (Law practice)	Material breach implicating the lawyer's confidentiality (Ariz. R. Sup. Ct. 42, ER 1.4 + ER 1.6(e); ABA Formal Op. 483).	Promptly, with sufficient detail to permit informed decisions

Service providers with access to Customer Information are contractually required to notify the Firm of any breach as soon as possible and no later than 72 hours after becoming aware.

6. Identity Theft Red Flags

The Firm maintains a written Identity Theft Prevention Program under SEC Regulation S-ID, 17 CFR § 248.201, to detect and respond to identity theft indicators in connection with covered accounts.

7. Recordkeeping

Each Incident is logged from detection through post-incident review. Records are retained for at least seven years and are accessible to the Responsible Person, Firm leadership, and counsel.

8. Testing and Training

- **Annual training exercises** led by the Responsible Person.
- **Annual review** of each critical service provider.
- **New-hire training** within 30 days of hire.
- **Annual refresher** for all personnel.

9. Annual Review

The Program is reviewed within 60 days of the anniversary of its effective date and after any material change to operations, technology, regulators, or applicable law. Material amendments are approved by the President.

This summary is provided for informational purposes. The underlying Program and the Firm's other compliance policies govern in all cases.