This is a comprehensive, theory-based response to the lab assignment. Due to the constraint of a single output, the content for the five required deliverables is presented sequentially with clear professional formatting. In a final submission, each Task's deliverable would be a separate, professionally formatted document adhering to the specified page limits.

GRC105 - Incident Management and Business Continuity

CRC100 – Incident Management and Business Continuity
Lab Assignment: Crisis Communication and Stakeholder Management
FinTrust Bank: Comprehensive Crisis Communication Program
Task 1: Crisis Communication Policy and Framework (25 points)
Deliverable: Crisis Communication Policy document (Conceptual Outline)
1.1 Policy Statement and Objectives
Policy Statement: FinTrust Bank Crisis Communication
It is the policy of FinTrust Bank to establish and maintain a proactive, ethical, and efficient crisis communication capability to protect the institution's customers, employees, reputation, and financial stability, and to meet all mandatory regulatory obligations during disruptive events. This policy ensures clear, consistent, and timely communication with all stakeholders in alignment with our core value of **Trust and Transparency**.
Component	Description
Purpose	To define the authority, structure, and operational framework for all internal and external communication activities during a crisis.
Scope	Applies to all FinTrust Bank employees, contractors, third-party partners, communication channels, and all events that threaten the bank's operations, reputation, or financial standing.
Commitment	**Executive Commitment:** The CEO and Board of Directors fully endorse this policy, commit the necessary resources ($500,000 budget, dedicated CCO role), and mandate its integration into the existing Incident Response (IR) and Business Continuity/Disaster Recovery (BC/DR) programs.
Alignment	Aligns with FinTrust's core values (Trust, Accountability, Customer-Centricity) and critical regulatory requirements (e.g., FDIC safety and soundness, OCC guidelines, GLBA customer data safeguarding, Federal Regulator notification).
Specific Program Objectives
Speed & Accuracy: Disseminate initial holding statements to critical stakeholders within $\mathbf{20}$ minutes of crisis confirmation and provide accurate, factual updates to all stakeholders at defined intervals (aligned with the $\mathbf{60-90}$ standard).
Reputation & Trust: Preserve and rebuild public trust and the organization’s reputation by demonstrating competence, concern, and corrective action (guided by $\mathbf{SCCT}$).
Compliance: Ensure all mandatory regulatory notifications (e.g., 36-hour rule for Federal Regulators on "notification incidents") are met with accurate, timely, and compliant communication.
Stakeholder Assurance: Provide targeted, relevant information to key stakeholders (customers, employees, investors) to minimize anxiety, prevent misinformation, and maintain operational stability.
Operational Support: Support the Incident Response (IR) and Business Continuity

Operational Support: Support the Incident Response (IR) and Business Continuity (BC/DR) teams by gathering stakeholder intelligence and communicating critical operational updates (e.g., branch closures, service restoration).
*
1.2 Crisis Definition and Classification Framework
Crisis Definition
A crisis for FinTrust Bank is defined as a significant, unexpected event that threatens to severely impact the organization's reputation, financial viability, customer/employee trust, and/or ability to comply with critical regulatory requirements, requiring immediate, non-routine communication and management intervention beyond standard incident response.
Crisis Classification System (Based on SCCT)
Crisis Cluster (SCCT)	Organizational Responsibility Attribution	Crisis Scenarios (FinTrust Examples)	Primary Response Strategy
Victim Crisis (Low Responsibility)	The organization is a victim; little to no responsibility.	Natural disaster (e.g., regional flood impacting HQ), external criminal act (e.g., DDoS attack), workplace violence, or malicious external data theft.	**Deny / Bolster:** Focus on sympathy, victimhood, and reminding stakeholders of past good deeds (ingratiation).
Accidental Crisis (Moderate Responsibility)	The organization's actions caused the crisis, but unintentionally and without malicious intent.	Technical error/system failure (e.g., core banking platform outage due to an untested patch), technical error product harm (e.g., erroneous credit card charge processing), or unintended human error.	**Diminish:** Focus on excusing (low-controllability factors) or justifying (good intentions) the incident.
Preventable Crisis (High Responsibility)	The organization intentionally took an inappropriate risk or violated a rule/law, or its operations were clearly negligent.	Organizational Misdeed (e.g., regulatory enforcement action due to lax AML/KYC controls), human error product harm (e.g., employee phishing scam that compromises customer data), or executive misconduct.	**Rebuild:** Focus on apology, compensation, and corrective action. May include a **Bolster** strategy.
Crisis Severity Levels
Level	Criteria & Impact	Activation & Escalation
Level 4 - Major/Catastrophic	Systemic failure (e.g., complete core banking outage > 48 hours), widespread data breach (millions of customers), material financial impact (>$50M), or regulatory mandate to suspend critical operations.
High/Immediate Reputation Threat.	Full Crisis Management Team (CMT) & Crisis Communication Team (CCT) activation. CEO-level spokesperson. 24/7 War Room. Immediate Regulatory/Law Enforcement notification.

Level 3 - High	Significant service disruption (e.g., mobile app outage > 12 hours), contained data breach (< 100k customers), significant financial loss (>$5M), or negative media coverage in all 8 states of operation. **Moderate Reputation Threat.**	CCT activated. Executive Spokesperson (COO/CISO). Regular, scheduled media and stakeholder updates. CMT lead notified.
Level 2 - Moderate	Localized service interruption (e.g., single branch closure due to power), minor data exposure (no financial harm), or localized negative social media trend. **Low Reputation Threat.**	CCT communication lead activated. Subject Matter Expert (SME) spokesperson. Manage locally/internally. Prepare for escalation.
Level 1 - Incident/Minor	Managed by routine Incident Response (IR). No immediate reputational threat or service impact beyond a few users.	Routine IR/Helpdesk/Branch communications protocols. CCO/CCT informed on a **monitor-only** basis.

Attribution Analysis Framework

Dimension	Description	SCCT Link
Internal vs. External	Did the cause originate within FinTrust's direct control (e.g., poor patch management, employee error) or from an external source (e.g., natural disaster, third-party vendor failure)?	Internal attribution increases organizational responsibility and reputational threat.
Intentional vs. Unintentional	Was the event a deliberate act (e.g., executive fraud, a malicious employee, known ignored risk) or an accident/error?	Intentional acts dramatically escalate the crisis to a **Preventable** cluster, mandating a **Rebuild** strategy.
Controllability	How much control did the organization have over the factors that led to the crisis?	Low controllability (e.g., global supply chain failure) moves the crisis toward an **Accidental** or **Victim** cluster.

*

1.3 Stakeholder Identification and Analysis

Complete Stakeholder Inventory

Internal	External	Regulated/Critical
Employees (3,500)	Retail Customers (2.5 million)	Federal Reserve, OCC, FDIC, CFPB
Managers/Supervisors	Business/Commercial Clients	State Banking Regulators (8 States)
Executive Leadership (CEO, CISO, CRO, COO)	Media (National, Regional, Industry)	Law Enforcement (FBI, Secret Service, State AGs)
Board of Directors	Investors/Shareholders/Analysts	Third-Party Vendors/Partners (e.g., core processor)
Crisis Communication Team (CCT)	General Public/Social Media Users	Insurance

Carriers (Cyber Liability) |

Stakeholder Prioritization (Power-Interest Matrix Application)

Quadrant	Stakeholders (FinTrust Example)	Engagement Strategy	Communication Requirements/Preferences
High Power / High Interest (Manage Closely)	**Regulators (Fed, OCC, FDIC, CFPB)**, **Board of Directors**, **Executive Leadership**, **Key Investors**, **Systemic Commercial Clients**.	**Priority 1:** Engage actively and frequently. Personal contact (phone/secure email). Compliance-focused, factual, and legally reviewed.	**Requirements:** Factual, timely, compliant notifications (e.g., $\mathbf{36-hour}$ rule). Detailed impact assessment, Root Cause Analysis (RCA), and remediation plan. Secure, auditable channels.
High Power / Low Interest (Keep Satisfied)	**Insurance Carriers**, **Law Enforcement**, **State AGs**, **Select Third-Party Vendors** (if not directly impacted).	**Priority 2:** Maintain regular contact. Keep them informed of decisions and potential impacts. Detailed communication on a need-to-know basis.	**Requirements:** Formal, documented, and concise updates. Focus on their specific interest (e.g., liability, legal cooperation, operational dependency).
Low Power / High Interest (Keep Informed)	**Retail Customers (2.5M)**, **All Employees**, **General Media**, **General Shareholders**, **Digital Platform Users (1.8M)**.	**Priority 3:** Proactive, mass communication. Use multiple, easily accessible channels. Focus on *Impact* and *What to Do Next*.	**Requirements:** Clear, empathetic, and consistent messaging (FAQ format). Use mass notification (email, website, social media). Focus on security, service restoration, and financial peace of mind.
Low Power / Low Interest (Monitor)	**General Public**, **Local Community Organizations**, **Suppliers (non-critical)**.	**Priority 4:** Minimal effort. Monitor for misinformation/sentiment. Use public channels (press release, website).	**Requirements:** General updates. Focus on organizational stability and community well-being.

Employee Stakeholder Segmentation and Communication Needs

Segment	Communication Need	Preferred Channel
Front-Line Staff (Branches/Call Center)	Real-time, clear talking points (what to say to customers), FAQ updates, and reassurance about their safety/jobs.	Manager briefings (mandatory huddles), Internal Crisis Intranet Portal, Secure Mobile App/SMS Alert.
Incident Response/BC/DR Teams	Technical facts, mission objectives, clear communication tasks, and external stakeholder sentiment/concerns.	Dedicated CCT-IR/BC Bridge Line, Secure Chat/Email, Shared Crisis Management Platform.
Executive Leadership	Key message approval, sentiment analysis summaries, media inquiry log, and regulatory compliance status.	CEO/CMO 1:1 briefing, CCT

media inquiry log, and regulatory compliance status. | SCC/Exec Briefing, SOC Dashboard/Status Report, Secure Executive Messaging. |
*

1.4 Governance Structure and Roles

Crisis Communication Team (CCT) Structure and Composition

The CCT reports directly to the **Chief Communications Officer (CCO)**, who serves as the CCT Lead, and operates in lockstep with the Crisis Management Team (CMT), led by the CEO/CRO.

Role	Title (FinTrust)	Responsibilities Summary
CCT Lead	Chief Communications Officer (CCO)	Strategic direction, final message approval (delegated by CEO), media relations, and SCCT strategy selection. Reports to CMT.
Internal Communications	VP, HR/Employee Communications	Employee notification, manager talking points, and monitoring internal sentiment/rumors.
External/Customer Comms	VP, Marketing & Digital Channels	Customer alerts (email, website, app), social media monitoring/response, and customer FAQ management.
Media Relations	Director, Public Relations	Managing all media inquiries, writing press releases, preparing spokespersons, and media monitoring/clipping.
Regulatory & Legal Review	Chief Legal Officer (CLO) Delegate	Ensuring all communications are compliant with GLBA, state laws, and regulatory notification requirements (CLO is part of the CMT, delegate works with CCT).
Technical Liaison	CISO/CSIRT Delegate	Real-time factual information flow from IR/BC/DR to the CCT. Vetting technical accuracy of all external statements.

RACI Matrix for Core Crisis Communication Activities

Activity	CCT Lead (CCO)	CEO/CMT Lead	CLO Delegate	Tech Liaison	Internal Comms	External/Customer Comms
Crisis Activation	**C** (Informed)	**A** (Authorizes)	**I** (Informed)	**I** (Informed)	**I** (Informed)	**I** (Informed)
Holding Statement Draft	**A** (Approves/Accountable)	**R** (Review)	**C** (Consult)	**C** (Consult)	**R** (Draft Internal)	**R** (Draft External)
Regulatory Notification	**R** (Responsible for Delivery)	**A** (Authorizes)	**A** (Accountable for Content)	**C** (Consult for Facts)	**I** (Informed)	**I** (Informed)
Spokesperson Authorization	**A** (Approves/Accountable)	**C** (Consult)	**I** (Informed)	**I** (Informed)	**I** (Informed)	**I** (Informed)
Website/App Status Update	**R** (Review)	**I** (Informed)	**C** (Consult)	**C** (Consult for Facts)	**I** (Informed)	**A** (Accountable/Responsible)

Escalation Criteria and Decision-Making Authority

Activation: The **CCO** can activate the CCT in **Level 2** or higher. The **CMT Lead (CEO/CRO)** must authorize **Level 3** and **Level 4** crisis declarations and all external

(CEO/CRO) must authorize **Level 3** and **Level 4** crisis declarations and all external communications to the media and regulators.
Decision Authority: *The **CCO** has full authority over* channel selection*,* timeline execution*, and* drafting of key messages* (Level 2). In Level 3/4, the **CMT Lead** has final sign-off authority on all external communication releases.
Information Escalation: The **Technical Liaison** must immediately escalate any information that changes the SCCT classification (e.g., discovering human negligence in an 'Accidental Crisis') or triggers a regulatory deadline to the **CCO** and **CLO Delegate**.
Spokesperson Designation and Backup Protocols
Crisis Type / Severity	Primary Spokesperson	Backup Spokesperson
Level 4 (Catastrophic)	Chief Executive Officer (CEO)	Chief Risk Officer (CRO)
Cybersecurity / Data Breach	Chief Information Security Officer (CISO)	CCO or CISO Backup
System Outage / BC/DR Activation	Chief Operating Officer (COO)	CCO or Head of Retail Banking
Regulatory / Legal Crisis	Chief Legal Officer (CLO) or CRO	CCO
Internal / HR Crisis	CCO or VP, Human Resources	Internal Comms Lead
Routine Media Inquiries	CCO or Director, Public Relations	Media Relations Lead
Protocol: Spokespersons must be trained (Task 4), adhere to approved talking points, and not speculate or comment on legal/compliance issues without the CLO's explicit approval. The backup is trained to assume the primary role with all delegated authority within 2 hours of the primary's unavailability.

Task 2: Crisis Communication Plan Development (30 points)
Deliverable: Crisis Communication Plan document (Conceptual Outline)
2.1 Activation and Notification Procedures
Activation Criteria for Crisis Communication Response (CCT)
CCT is formally activated when:
Incident Status Change: The Incident Response Team (CSIRT) or BC/DR Team declares a **Level 2** incident or higher (potential for reputation damage, financial loss, or major service disruption).
Regulatory Trigger: A "Notification Incident" (as defined by US Federal Regulators) is determined, mandating a $\mathbf{36-hour}$ notification.
Media/Social Spike: Uncontrolled, negative media or social media activity related to FinTrust Bank that threatens stability or trust.
Notification Protocols and Contact Trees
Primary System: Dedicated Crisis Management Platform (e.g., mass notification system) for all CCT/CMT/IR/BC/DR personnel. **Channel 1:** SMS Alert, **Channel 2:** Automated Voice Call, **Channel 3:** Crisis Email.

After-Hours/Weekend Activation: System automatically triggers all CCT/CMT personnel upon Level 2+ declaration by the on-call incident manager. The CCO is automatically notified by the CISO/CRO on-call executive.
Assembly Procedures: CCT members must acknowledge the alert within **5 minutes**. The team is instructed to immediately join the dedicated, pre-established virtual "War Room" (Secure Video/Bridge Line) and access the Crisis Management Platform for initial facts and holding statement drafts.
Integration with Incident Response (IR) and BC/DR Activation
Single Trigger Point: *The IR/BC/DR's Level 2+ incident declaration* simultaneously* triggers CCT activation and the **Technical Liaison's** immediate task to provide initial facts to the CCO.
Information Hand-off: Technical facts (what happened, current impact, recovery status, estimated time to recovery) flow from IR/BC/DR to the CCT's Technical Liaison. The CCT's Communication Status Report flows back to IR/BC/DR leadership.
*
2.2 15-20-60-90 Minute Response Timeline
This timeline begins at **T+0:00**, the moment the CCT Lead (CCO) confirms the crisis and authorizes the start of the communication response.
Time Milestone	Key Actions	Responsible Roles	Output / Deliverable
T+0:00 to T+0:15 (First 15 Minutes)	**Initial Assessment & Internal Notification**	**Technical Liaison, CCT Lead (CCO)**	**Internal CCT Activation & Fact Sheet.**
T+0:15 to T+0:20 (20 Minutes)	**Stakeholder Notification & Holding Statement**	**CCO, CLO, External/Customer Comms**	**Internal Employee Alert** (minimal facts, status: "Incident Confirmed, CCT Activated"). **Generic Holding Statement** approved and posted to the dark site.
T+0:20 to T+0:60 (60 Minutes)	**Comprehensive Initial Statement & Stakeholder Updates**	**CCO, Media Relations, CLO, Technical Liaison**	**Comprehensive Initial Statement** (incorporating SCCT strategy, situation summary, current actions, and *commitment to updates*). **Targeted Customer Email/App Push**. **Regulatory Team Briefing** (on facts known so far).
T+0:60 to T+0:90 (90 Minutes)	**Media Engagement & Ongoing Communication Rhythm**	**Media Relations, Primary Spokesperson, CCO**	**Press Release** distributed to key media. **Spokesperson prepped** for media calls/briefing. **Social Media FAQs** posted. **Decision:** Is a press conference needed? Set **Next Update Time** (e.g., T+4:00).
T+0:90+ (Ongoing)	**Sustained Communication**	**All CCT**	Regular updates to all stakeholders at committed intervals. Sentiment monitoring and After-Action Review (AAR) preparation.
*
2.3 Communication Channels and Protocols

Stakeholder Group	Primary Channel	Backup Channel	Channel Selection Criteria
Employees	Internal Crisis Intranet Portal, SMS Alert System	Manager Briefings/Huddles, Personal Email (off-network)	Speed, ability to confirm receipt, security (in case of network outage).
Customers (Retail)	Secure FinTrust Website/App Status Page, Email Notification	Social Media (verified accounts), Branch Signage, Toll-Free Hotline	Reach, ability to provide security/privacy reassurances, auditability.
Regulators/Law Enforcement	Secure Regulatory Portal, Pre-approved Formal Email (from CLO)	Secure Phone Call, In-person Briefing	Formality, compliance, security, and record-keeping (audit trail).
Media/General Public	Press Release (Wire Service), Dedicated News/Status Page, Spokesperson Interview	Verified Social Media Accounts (X, LinkedIn), Dark Site Activation	Speed, control of narrative, broad reach.
Investors/Shareholders	Investor Relations Portal, SEC Filing (if material), Dedicated Email	Analyst Call, CEO Statement Video	Formality, regulatory (SEC) compliance, sensitivity to material non-public information.

Social Media Protocols and Approval Processes

Monitor & Listen: Immediately activate 24/7 social media listening for key terms, misinformation, and public sentiment.

Pause Non-Crisis Content: Halt all scheduled marketing and promotional posts immediately upon Level 2+ activation.

Approve: All social media posts and direct responses *must* be drafted by the External/Customer Comms Lead, reviewed by the **CCO**, and cleared by the **CLO Delegate** prior to posting.

Respond: Use pre-approved **Holding Statement** and **FAQ** content only. Do not engage in speculation, arguments, or assign blame. Redirect users to the official FinTrust Website/App Status Page.

Dark Site: Activate a pre-built, secure, and resilient "dark site" (a hidden section of the public website) that is immune to core system outages to host all crisis communications.

*

2.4 Message Development Framework

Message Development Process and Approval Workflow

Fact Gathering: Technical Liaison provides verified facts to CCT Lead.

SCCT Strategy Selection: CCO determines the SCCT crisis cluster and selects the appropriate primary response strategy (Task 2.5).

Drafting: Internal and External Communications Leads draft messages using the **Key Message Framework Template**.

Legal/Regulatory Review: Drafts sent to the **CLO Delegate** for clearance on compliance, liability, and regulatory notification alignment.

Executive Approval: Final drafts are reviewed and approved by the **CMT Lead (CEO/CRO)**.
Dissemination: CCT Lead authorizes distribution across all selected channels.
Key Message Framework Template
Element	Purpose	Placeholder/Guidance
Acknowledgment & Concern	Show empathy and confirm the crisis.	**[Acknowledge the situation]**. We understand the severity of this. The safety of our customers and the security of their assets are our top priority. (Always mandatory)
Facts Known (S.A.I.)	Situation, Action, Impact. Be transparent.	**[Situation Summary]** e.g., "A technical system error has caused..." **[Current Actions]** e.g., "Our teams are working 24/7 to..." **[Impact Assessment]** e.g., "There is **no evidence** of customer data compromise."
SCCT Core Strategy	The one sentence that drives reputation.	**Victim/Accidental:** "We are taking every measure to contain this external attack and support all affected clients." **Preventable:** "We take full responsibility and sincerely apologize for this error. We are committed to compensation and fixing the root cause."
Stakeholder Guidance	What do they need to *do*?	**[Customer Guidance]** e.g., "Do not click on unverified links." **[Employee Guidance]** e.g., "Refer all media inquiries to the CCO's office."
Next Update	Set expectation and control the information cycle.	**We commit to providing our next update at [Date/Time] via [Channel].**
Tone and Voice Guidelines:
Victim Crisis: Empathetic, Reassuring, Competent.
Accidental Crisis: Serious, Accountable, Transparent.
Preventable Crisis: Remorseful, Responsible, Corrective.
Consistency Mechanisms:
All spokespersons and communication leads must use the approved **Talking Points Format** and refer to the official **Crisis Status Report** on the CCT Platform.
The **Media Relations Lead** must perform a "Message Audit" check against all internal and external releases before the T+60 milestone.
*
2.5 SCCT Response Strategy Selection
SCCT Strategy Selection Matrix (Mapping Crisis Types to Response Strategies)
The selection is based on the crisis cluster (severity of reputational threat) and any mitigating factors (e.g., strong prior reputation, no prior crisis history).
Crisis Cluster (Reputational Threat)	Primary SCCT Strategy (Required)	Secondary/Optional Strategies
Victim Crisis (Lowest Threat)	**Deny** (Denial, Attack Accuser, Scapegoat - *if third party is truly responsible*)	**Bolster** (Reminder, Ingratiation, Victimage) - Use to

party is truly responsible). | **Bolster** (Reminder, Ingratiation, Victimage) - Use to reinforce FinTrust's positive work. |
| **Accidental Crisis** (Moderate Threat) | **Diminish** (Excuse - *minimize harm/intent*; Justification - *good intention*). | **Bolster** (Reminder of past good works) - Use to increase positive reputation buffer. |
| **Preventable Crisis** (Highest Threat) | **Rebuild** (Full Apology, Compensation). **Corrective Action** (Mandatory - show steps to prevent recurrence). | **Bolster** - Use only *after* Rebuild strategy has been executed. |

Decision Framework for Strategy Selection

Question	Yes $\rightarrow$ Action	No $\rightarrow$ Action
Was the organization to blame? (Internal/Controllable?)	Move to Diminish/Rebuild.	Move to Deny/Bolster (Victim).
Was the act intentional or negligent?	**MANDATE REBUILD STRATEGY** (Full Apology & Compensation). Level 4 crisis likely.	Move to Diminish (Accidental).
Are there significant mitigating factors (e.g., force majeure, 3rd party failure)?	Use **Excuse** (Diminish) to shift focus to low controllability.	Acknowledge greater responsibility.
Is the organization a repeat offender?	**MANDATE FULL REBUILD** regardless of cluster (prior history increases reputational threat).	Select strategy based on the initial cluster.

Example demonstrating Strategy Application

Scenario	SCCT Cluster	SCCT Strategy	Key Message Focus
Ransomware Attack on Third-Party Payroll Vendor	**Victim** (Malicious External)	**Deny + Bolster**	"We are the victim of a sophisticated criminal attack targeting our vendor, [Vendor Name]. We regret the impact, but want to remind our customers that *their* FinTrust accounts remain safe, thanks to our robust internal security."
Core Banking System Outage due to Untested Update	**Accidental** (Technical Error Accident)	**Diminish + Excuse**	"We are experiencing a system disruption following a routine maintenance process. We sincerely apologize for the inconvenience. This was an unintended error; our teams are focused on full restoration within X hours. No customer funds or data were at risk."
Regulatory Fine for Misleading Mortgage Lending Practices	**Preventable** (Organizational Misdeed)	**Rebuild + Corrective Action**	"We take full responsibility and sincerely apologize to our customers. We accept the findings of the regulator and are committed to [Compensation/Remediation Action]. We are overhauling our entire lending compliance framework to ensure this never happens again."

Task 3: Communication Templates and Tools (20 points)

Deliverable: Communication Templates Package (Conceptual Structure)

All templates use placeholders in [BRACKETS] for information that must be inserted

All templates use placeholders "[BRACKETS]" for information that must be inserted and reviewed by the CLO. **Instructions for Use** are mandatory.

3.1 Holding Statement Templates (4 points)

Instruction for Use: *Select the most relevant template, insert only the bracketed information, obtain CCO/CLO clearance (verbal approval is sufficient in T+0:20), and disseminate immediately to all employees, key regulators, and the public status page.*

Template Name	Placeholder/Mandatory Content
Generic Holding Statement (Immediate Use)	FinTrust Bank confirms we are aware of **[brief description of incident/rumor]**. Our Crisis Management Team is actively engaged and investigating the situation. **[Commitment/Action]**: Our first priority is to contain the issue and protect our customers. **We will provide an official statement and verified update at [Time/Interval]** via our website status page.
Scenario: Data Breach/Cybersecurity Incident	FinTrust Bank has detected a **[Type of Incident, e.g., unauthorized access/cyber incident]**. We have activated our full Incident Response Team (CSIRT) and notified law enforcement. **Initial assessment indicates [Impact, e.g., no immediate risk to customer funds/no evidence of customer data compromise]**. We are working with **[External Forensics Firm Name]** to confirm the scope. **We commit to providing a detailed update on the scope of impact and customer guidance within the next [Time/Interval]**.
Scenario: System Outage/Service Disruption	FinTrust Bank is experiencing a **[Service Affected, e.g., widespread system outage impacting online/mobile banking]**. Our technical teams are working with extreme urgency to resolve the issue. We understand the inconvenience and apologize. **We are [Action, e.g., rerouting transactions/activating BC plan] to restore services. Our branches remain [Status, e.g., open for essential services]. Next update: [Time/Interval]**.
Scenario: Regulatory Investigation	FinTrust Bank acknowledges receipt of an inquiry from **[Regulatory Agency Name]** regarding **[General Subject Area, e.g., a specific operational matter]**. We are fully cooperating with the investigation. **As a regulated institution, we are unable to comment on the details of an ongoing inquiry.** Our core operations and customer services remain unaffected. **We will provide a statement on the resolution once permitted.**
Scenario: Employee Safety Incident	FinTrust Bank confirms an incident occurred today at our **[Location/Branch Name]**. All employees and customers are safe and accounted for. **[Action]**: Local authorities are on site, and the **[Location]** is temporarily closed. **Our thoughts are with [mention affected party, if appropriate].** Further information will be shared with employees via internal channels at **[Time/Interval]**.

3.2 Comprehensive Statement Templates (5 points)

Instruction for Use: *To be used at the T+60 and T+90 milestones. **SCCT Strategy** must be integrated into the tone and content (e.g., apology is mandatory for*

Preventable).

Template Name	Key Sections / SCCT Integration
Full Statement: Data Breach/Cybersecurity (Victim/Accidental)	**Situation Summary:** Verified facts, date/time discovered, current status (contained/not contained). **SCCT Integration (Deny/Diminish):** Strong statement on FinTrust as a **victim** or that the cause was a **complex technical error (excuse)**. **Impact Assessment:** Explicitly state: "We have confirmed that **[Number]** customer records were potentially exposed." **Response Actions:** Steps taken (forensics, systems hardening, law enforcement notification, $\mathbf{36-hour}$ regulatory notification). **Stakeholder Guidance:** Clear instructions on what customers must do (e.g., monitor accounts, sign up for free credit monitoring via **[Vendor Name]**). **Contact Info & Next Steps:** Dedicated hotline and commitment to next update.
Full Statement: System Outage/Disruption (Accidental)	**Situation Summary:** Detail on *which* service is down (Mobile/Online/Branches) and the current technical cause (e.g., technical upgrade failure). **SCCT Integration (Diminish/Justification):** Apology, followed by a **justification** that the failed upgrade was intended to improve security/service (good intentions). **Response Actions:** RTO (Recovery Time Objective) and RPO (Recovery Point Objective) update. Activation of BC/DR plans (e.g., manual processes, alternative service points). **Stakeholder Guidance:** How to perform essential banking functions in the interim (e.g., using ATMs, visit open branches, payment flexibility). **Internal-Specific Section:** Manager talking points on customer reassurance and fee waivers.
Full Statement: Regulatory Investigation (Preventable)	**Situation Summary:** Confirmation of the regulatory action and the subject (e.g., fine, consent order). **SCCT Integration (Rebuild/Apology):** Unambiguous, sincere **apology** and full acceptance of responsibility. **Response Actions: Corrective Action** details (e.g., hiring a new CLO, retraining all staff, implementing a new compliance system). **Remediation & Compensation:** Specifics on how affected customers will be identified and compensated/reimbursed. **Regulator-Specific Version:** Attachments with detailed compliance and remediation plans.

3.3 Internal Communication Templates (4 points)

Template Name	Purpose & Key Content
Employee Notification Email Template	**Subject:** URGENT: FinTrust Bank Official Internal Update – Incident **[Incident ID]**. **Content:** $\mathbf{T+15}$ Acknowledgment. Reassure staff. Provide key talking points for customer interaction (what *can* be said). Direct all media inquiries to the CCO's office. Provide internal FAQ link.
Manager Talking Points Template	A two-column document. **Column 1 (The Question/Rumor):** What is the customer/employee asking? **Column 2 (The Approved Answer):** Use the pre-approved Key Message Framework. **Instruction:** *Managers are*

prohibited from deviating from these points. Must be updated at T+60 and every 4 hours thereafter. |
| **Intranet Crisis Update Template** | **Format:** A simple, high-contrast digital bulletin. **Sections:** 1. Current Status (Green/Yellow/Red). 2. System Status (which systems are up/down). 3. **Employee Guidance** (e.g., working from home/alternative site). 4. Next Internal Town Hall time. |
| **Town Hall Presentation Template** | **Structure:** 1. CEO/Executive Message (Empathy & Gratitude). 2. Facts and Status (CISO/COO). 3. Q&A (CCO-managed, using manager talking points). 4. $\mathbf{SCCT}$ Strategy (Reputation Rebuild/Assurance). 5. Thank you and Next Steps. |
3.4 External Communication Templates (4 points)
Template Name	Channel / Key Audience	Key Content / Goal
Customer Notification Template (Email & Website)	Customers (2.5M)	Personalized salutation. SCCT-aligned message. **Call-to-Action** (e.g., check your statement). Reassurance on GLBA and data protection. Must be clear, short, and non-jargon.
Press Release Template	Media (Regional/National)	AP style. Headline must reflect SCCT strategy (e.g., "FinTrust Reassures Customers After External Cyber Incident" vs. "FinTrust Apologizes, Takes Responsibility for Error"). Quote from the Primary Spokesperson. Boilerplate background on FinTrust.
Social Media Post Templates (X/LinkedIn)