Business Continuity Plan

Version: XTENDBCP-v20221031

***Confidentiality Statement**: This document contains sensitive information regarding the operations of Xtend and the CU*Asterisk partner network. It may not be distributed without the consent of the Xtend Executive Team.*

Plan Contents

NOTE

Data and information contained within this Plan (where applicable) has been provided by Xtend and CU*Answers in the form of electronic files/documentation and as the result of notes taken during conversations with key personnel. It is the responsibility of the Credit Union to maintain this Plan to ensure contents are accurate and current.

Introduction

This document is designed for the purposes of equipping and preparing Xtend and its partners for the expected impact of unplanned disruptions to business functions and processes and for contributing to the resiliency of operations.

The Xtend Business Continuity Plan is "a roadmap for continuing operations under adverse conditions (i.e., interruption from natural or man-made hazards)". The Plan is the primary tool used for preparedness training, testing, and exercising. The best investment in business continuity management is a well-trained recovery team. The Plan should be studied, and its contents well known prior to the next disruption.

Portions of the CU*Answers Business Continuity Plan are included in the contents of this plan to support the recovery effort where appropriate.

Scope and Objectives

A disaster is a unique event, and the provisions of this plan can be used as the basis for controlling specific recovery operations at management's discretion. Execution of this plan will help facilitate the timely recovery of core processing critical business functions.

The core framework of this plan was developed with the following objectives:

- To protect personnel and property (assets)
- To minimize the financial losses to the organization
- To serve clients with minimal disruptions
- To mitigate the negative effects of disruptions on business operations

The procedures contained within have been designed to serve as a guide for responding to emergencies based on recognized standards and best practices, written with the FFIEC published recommendations in mind. Details about these recommendations can be found at the FFIEC website or at http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning.aspx.

Confidentiality Statement

This plan is strictly confidential and is not to be shared with anyone outside the CU*Asterisk network without the express permission of the President/CEO. Full copies of the current plan are kept by each management team member. All questions from the news media or other external sources regarding the plan or any disaster/incident should be directed to the Incident Manager or CEO.

*See "Crisis Communications" section.

Assumptions

The following assumptions have been considered during the creation of this recovery plan. The specific circumstances of any disruption may require modifications to the recovery effort.

- Key personnel have been identified and trained and are available to activate the recovery plan.
- Current backups of the application software and data are intact and available at a quickly accessible storage facility.
- Service agreements are maintained with the application hardware, software, and communications providers to support the emergency system recovery.

Plan Maintenance

The Xtend Business Continuity Plan will be revised every twelve months or as needed based on:

- Changes in potential threats or risks,
- Considerable changes in business operations, functions, or processes,
- Considerable changes in system or network architecture,
- Audit recommendations,
- Lessons learned from tests, exercises, and events.

Revised plans will be distributed to all Emergency Response Team personnel, Board members and staff with direct roles and responsibilities within the plan. General information about the Continuity Plan and program may be referenced on the corporate web site and a sanitized version of the plan available to client credit unions upon request.

Revised on (Date)	Revised by:	Notes	Board Acceptance (Date)
8/14/2014	L. Winninger/ J. Lawrence	Initial draft for review	11/15/2014
8/11/2015	L. Winninger/ J. Lawrence	Annual refresh	8/31/2015
4/18/2016	L. Winninger/ J. Lawrence	Annual refresh	4/28/2016
3/14/2017	L. Winninger/ J. Lawrence	Annual refresh	3/23/2017
8/22/2018	L. Winninger/ D. Caliendo	Annual refresh	11/5/2018
9/27/2019	L. Winninger/ D. Caliendo	Annual refresh	10/24/2019
9/23/2020	L. Winninger/ D. Caliendo	Annual refresh	10/22/2020
9/21/2021	L. Winninger/ D. Caliendo	Annual refresh	10/28/2021
10/31/2022	L. Winninger/ P. Schumaker	Annual refresh	11/16/2022

Awareness and Training

To ensure all personnel are knowledgeable of the Plan and aware of their roles during a recovery effort, Xtend will commit a portion of annual management and staff meetings for educating employees as part of the ongoing Business Continuity Planning Cycle. In addition, training events and exercises for those with specific roles and responsibilities will be conducted as needed, particularly when any plan modifications have been made.

Training events will be documented and reported to the board annually.

Testing and Exercising

Recovery Plans (or portions thereof) are to be tested regularly to:

- Ensure completeness and accuracy of the procedures within the plan.
- Identify area within the plan that are weak and require modifications to improve plan effectiveness.
- Provide training and practice for recovery teams.
- Demonstrate (building confidence in) our ability to recover critical functions meeting acceptable time objectives.

Types of testing may include:

- **Life safety exercises**
  - Examples are building evacuation or shelter-in-place drills.
- **Plan walk-through/tabletop reviews**
  - Example is a plan review/walk-through with recovery team member(s) in a conference/meeting room environment.
- **Stand-alone exercises**
  - Recovery/relocation of a single business unit/department, single process/function, or single device/system.
  - An example would be testing VPN backup data communications to simulate an outage of the primary data communications line.
- **Comprehensive exercises**
  - A large-scale recovery effort such as rolling core-processing from the primary datacenter to the secondary datacenter.

All Xtend departments currently participate in CU*Answers recovery tests and some preparedness exercises.

*Results of the HA rollover tests are published at: https://www.cuanswers.com/solutions/business-continuity/auditing-and-testing/

Executive Commitment

Board and senior management responsibilities in Business Continuity Planning include:

- Establishing policy by determining how the institution will manage and control identified risks.
- Allocating knowledgeable personnel and sufficient financial resources to properly implement the Business Continuity Plan.
- Ensuring that the Business Continuity Plan is independently reviewed and approved at least annually.
- Ensuring staff are trained and aware of their roles in the implementation of the Business Continuity Plan.
- Ensuring the Business Continuity Plan is regularly tested on an enterprise-wide basis.
- Reviewing the Business Continuity Plan testing program and test results on a regular basis.
- Ensuring the Business Continuity Plan is continually updated to reflect the current operating environment.

Corporate Environment

Xtend is a multi-owned Credit Union Service Organization (CUSO) that provides clients with a variety of strategic products, services, and partnerships. Xtend's corporate mission is to increase client's competitive advantage by providing the highest quality products and services at an affordable price.

Founded in 2002, Xtend's Board of Directors consist of credit union executives with a common vision of helping their industry peers stay relevant in the eyes of their members in an increasingly competitive marketplace. This vision translates simply – provide the highest quality service at a price point that sets us apart. Xtend's corporate value proposition focuses on four main objectives: communication, collaboration, connection, and execution, with an overlying spirit of innovation that encompasses everything they do. By aligning Xtend's goals with their clients' business plan, they hope to help redefine the credit union's vision of what it means to be partners vested in each other's success.

Key Products and Services provided by Xtend include:

Bookkeeping

- Base Services
  - Daily Share Draft, ACH, and ATM reconciliation, settlement, and exception reporting.
- Stand-in Support
  - Short-term back-office support for holidays, vacations, and staff shortages.
- 5300 Call Report Services
- CU*BASE Conversion/De-conversion Support
- Lockbox Services

Mortgage/Loan Servicing (Lender*RE)

- Investor Reporting and Escrow Administration
  - Reconciliation, escrow analysis and payment, agency reporting for Fannie Mae, Freddie Mac and FHLB portfolio loans.
- Portfolio Conversion
  - Project management for conversions of portfolio from third-party service to CU*BASE.

E-Communications Services

- Member Reach
  - Targeted electronic messages to members based on a predefined schedule of activities.

- RevGen
  - Loan campaign solution, combining E-Marketing, and outbound call campaign to targeted members.

- Data Analyst
  - Data mining and CU*BASE tracker creation handled by Xtend; member calls made by the credit union staff.
- HTML eStatement Notifications
  - Interactive eStatement notifications.
- eNewsletter Service
  - Publication of monthly online eNewsletter delivered to members via email.
- OLLE
  - Contest lead generation app for credit unions, OLLE generates inbound leads.
- Digital Marketing
  - Digital Marketing offering including social management, online advertising, and retail offerings.

Contact Center Services

- Branch XT
  - Inbound member service provided during Xtension business hours through overflow, after-hour and/or fully engaged inbound Contact Center.
- Branch ST
  - Targeted outbound calls to members based on predefined schedule of activities.
- Core Direct
  - Loan application submission directly through the CU*BASE software.
- CU*BASE Conversion Support
  - Inbound member support, outbound member contact.
- Xtension Stand-In Support
  - Inbound member service designed to provide the possible support during significant branch outages (i.e., disaster recovery).
- Online Chat
  - Live Chat link deployed within It's Me 247 and/or on the credit union's website with interactions handled by Xtension agents.

Partner Support Services

- Shared Branching
  - Marketing and oversight of the CU*BASE shared branching network.
- Digital Signage
  - Digital signage content creation and delivery through cloud-based managed solution.
- Two-Way Texting
  - Eltropy platform that provides two-way texting support directly from the clients' landline.

Xtend is an active member of the CU*Asterisk network.

Operational Environment

Xtend operates out of a leased facility, located at:

2900 Charlevoix Dr SE – Suite 200
Grand Rapids, MI 49546

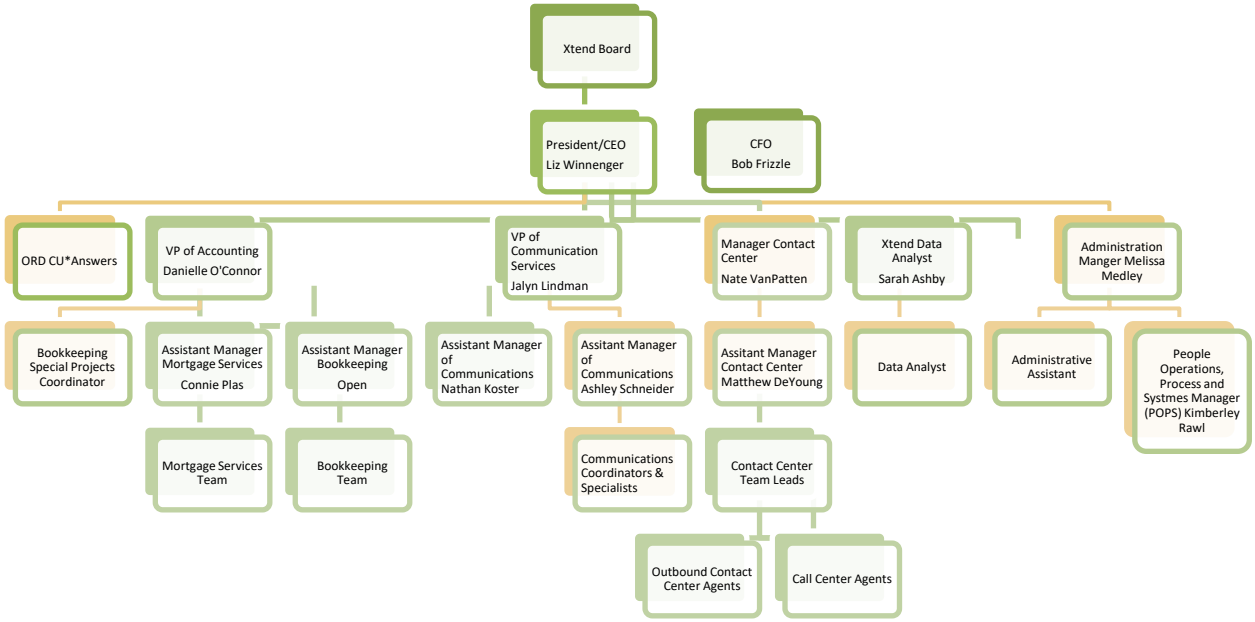
Xtend employs 75 staff members (mix of full and part-time) and serves 200+ credit unions.

Hours of operation include:

Monday – Friday	8:00 AM to 11:00 PM
Saturday	8:00 AM – 5:00 PM

Xtend Organizational Chart

(As of October 31, 2022)



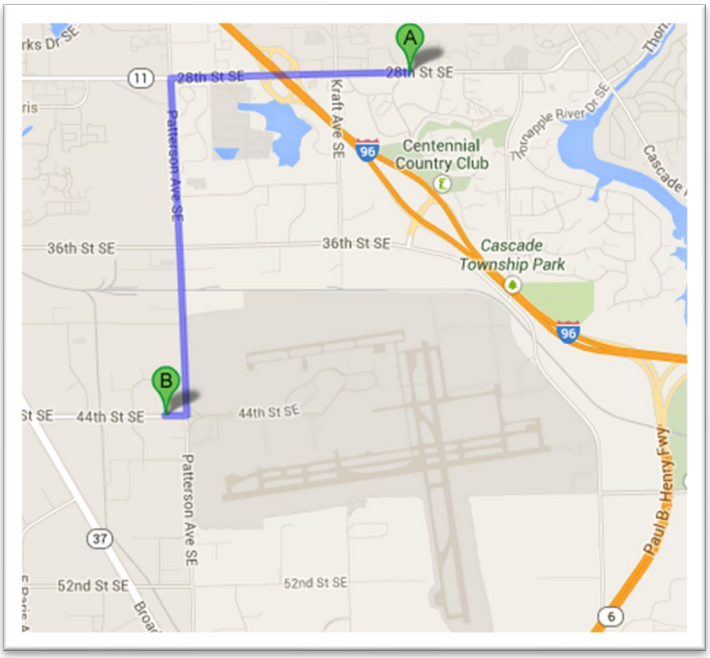
CU*Answers

Like Xtend, CU*Answers is a CUSO and CU*Asterisk network partner. CU*Answers maintains two locations in Michigan and is the primary developer and vendor for CU*BASE/GOLD software. In addition to the corporate offices in Grand Rapids, MI, CU*Answers maintains a primary production datacenter in Kentwood, MI and secondary high-availability datacenter in Yankton, SD.

[A]
CU*Answers Corporate Office
6000 28th street SE
Grand Rapids, MI 49546
800-327-3478
x132 Operations (24x7)
x266 Network Services

[B]
CU*Answers Production Datacenter
4695 44th street SE
Kentwood, MI 49512
800-327-3478

[not shown]
Site-Four
CU*Answers HA Datacenter
608 Goeden Dr.
Yankton, SD 57078
605-689-4309



CU*Answers provides CU*BASE/GOLD core processing and many of the complementary products and services used by Xtend staff and clients including:

- It's Me 247 Home and Mobile Banking
- Corporate Email (Exchange)
- VoIP Phone System
- Corporate Web Site
- Internal Portal
- AnswerBook
- Move IT
- Imaging Solutions
- Lync Communicator
- Web Chat
- Internal File/Print Server

In addition, Xtend has contracted CU*Answers to provide support for critical business functions from many departments including:

- IT Support (network/system administration, programming, security, etc.)
- Client Services
- Crisis Communications (alerts, announcements, etc.)
- Sales Support
- Marketing (web, etc.)
- Compliance/Legal
- Accounting
- HR/Administration

CU*Answers maintains a separate Business Continuity Program with regular recovery testing. Information about the CU*Answers program including reports from recovery exercises and test can be found at: https://www.cuanswers.com/solutions/business-continuity/auditing-and-testing/

Recovery at a Glance

Given the relationship with CU*Answers and the shared resources necessary to perform most of Xtend's critical business functions, all recovery efforts will require close coordination and communication between all recovery teams.

Possible scenarios considered for the purpose of this plan include:

- Loss of site or denial of access (no physical access to one or more sites)
- Loss of critical functions (service, department, vendor, supplier, etc.)
- Loss of power or other services (utilities, cooling, etc.)
- Loss of critical equipment (hardware/software)
- Loss of communications (data, voice)
- Loss of skilled personnel (injury, illness, pandemic)
- Breach of security (network/system compromise)

It's important to recognize that each incident is unique and requires careful assessment and an appropriate and coordinated response. Not every incident has the capacity to disrupt business functions, but every incident has the potential to create an impact.

Key factors to consider when making decisions during an incident include:

- Safety of all personnel (evacuation, shelter, etc.)
- Security of data
- Availability of core services, including timing, expected duration of outage, etc.
- Proactive monitoring and controls to detect potential additional disruptions and to alert recovery staff
- Accurate initial assessment to enact proper plans and minimize downtime
- Existing service level agreements with clients and vendors
- Client and vendor expectations
- Each plan's inherent lead time (preparation, chasing down tapes, travel, etc.)
- Importance of the first few minutes and hours of an event
- Potential FUD factor (fear, uncertainty, doubt) of recovery teams, chaos during initial stages, remain calm
- The status of the work in progress at the time of the disruption

Several controls have been implemented during day-to-day operations in an effort to prevent, manage, control, and mitigate the impact of identified risks. During a disruption, additional inherent security risks must be considered such as:

- Reduced fault tolerance during the recovery
- Reduced redundancy of data during the recovery
- Compounded failures (snowball/domino effect, uncontrolled events have a tendency to escalate)
- Physical/network security at alternate sites
- Recovery team fatigue during lengthy recovery efforts

Additional financial considerations include:

- Lost revenue from service outage
- Need for temporary (skilled) staffing
- Equipment rental during the recovery efforts
- Extra shipping costs for moving equipment and materials
- Travel/lodging expenses for recovery teams and displaced staff
- Legal obligations for deadlines missed and service level agreements not met
- Overtime costs (labor) for staff and vendors
- Reputation/brand image (potential future revenue)

The sequence of events described below provides a summary of the reaction and recovery process to a disaster. It is designed to help management keep perspective amid the crush of details and problems that occur during the disaster and to educate staff who are not regularly involved in the disaster planning process.

The "Emergency Response Team" (identified elsewhere in this document) is responsible to coordinate an assessment of the situation as quickly as possible. The purpose of this assessment is to identify the scope of the disaster. Specific areas that must be evaluated are the condition and availability of staff members, condition and availability of facilities and the condition of key computer and business systems.

Steps for a typical disaster recovery effort include:

1. **Incident detected**
    a. Invoke Emergency Response Plan if required.
    b. Perform initial response to mitigate risk (fire extinguisher, fire alarm, power down, etc.).
    c. Evacuate premise or seek safe shelter if necessary.
    d. Call local authorities (911 or as appropriate).

2. **Establish chain of command**
    a. A clear chain of command strategy should be determined prior to a disaster to anticipate scenarios where communication channels and/or select management team members are not available. It is important that this does not create a delay in key decision making, especially during the early stages of a recovery.

3. **Assess situation**
    a. A quick and accurate assessment is required. Consider elements of the incident such as:
        i. The availability and condition of staff members
        ii. The condition and availability of facilities
        iii. The condition of key computer and business systems and vital records.
    b. Engage additional Emergency Response Units if needed (Fire, Police, EMT, etc.).
    c. Escalate the incident if necessary.

4. **Declare crisis severity based on assessment (escalate)**
    a. Consider scope and duration of disruption based on the results of the assessment.
    b. Escalate based on scope and expected duration of outage (examples shown below):
        i. 0-24 hours (Disruption)
        ii. 24-96 hours (Emergency)
        iii. 96+ hours (Disaster)

5. **Establish command and control of incident and recovery effort**
    a. Setup command post (surviving site or other designated location).
    b. Determine appropriate response to contain incident and initiate recovery plan both during and after business hours.

6. **Notify recovery team members**
    a. Communicate to recovery team members the description of the incident, extent of damage, recovery location and prioritized action plan based on the circumstances of the incident.
    b. Invoke Contingency Plans if conditions warrant.
    c. See "Emergency Response Team" section for recovery team leaders' contact information.
    d. See "Appendix" for all-staff contact information.
    e. Mobilize teams to alternate recovery location(s) if required.

7. **Notify key stakeholders (members, vendors, media, etc.)**
    a. See "Crisis Communications" section of Plan.
        i. Send CU*BASE Alert and Announcement (or request CU*Answers to issue)

8. **Recover critical business functions**
    a. Consider alternate recovery strategies based on circumstances of disruption.
    b. Document and log recovery efforts including personnel hours worked.
    c. Monitor and control all disaster recovery related expenses.
    d. Provide status report to all recovery teams.

9. **Notify Insurance Claims Adjustor**
    a. Notify Lighthouse Insurance Group.

10. **Recover remaining business functions**
    a. Provide status report to all recovery teams and key stakeholders.

11. **Repair/replace facilities and systems (coordinated with CU*Answers)**
    a. Direct and control all salvage efforts related to facilities and vital records.
    b. Coordinate the restoration / building of permanent location.
    c. Procure replacement equipment and supplies as necessary.
    d. Schedule move back to main location.

12. **Return to permanent location**
    a. Resume normal operations.
    b. Provide status report to all key stakeholders.

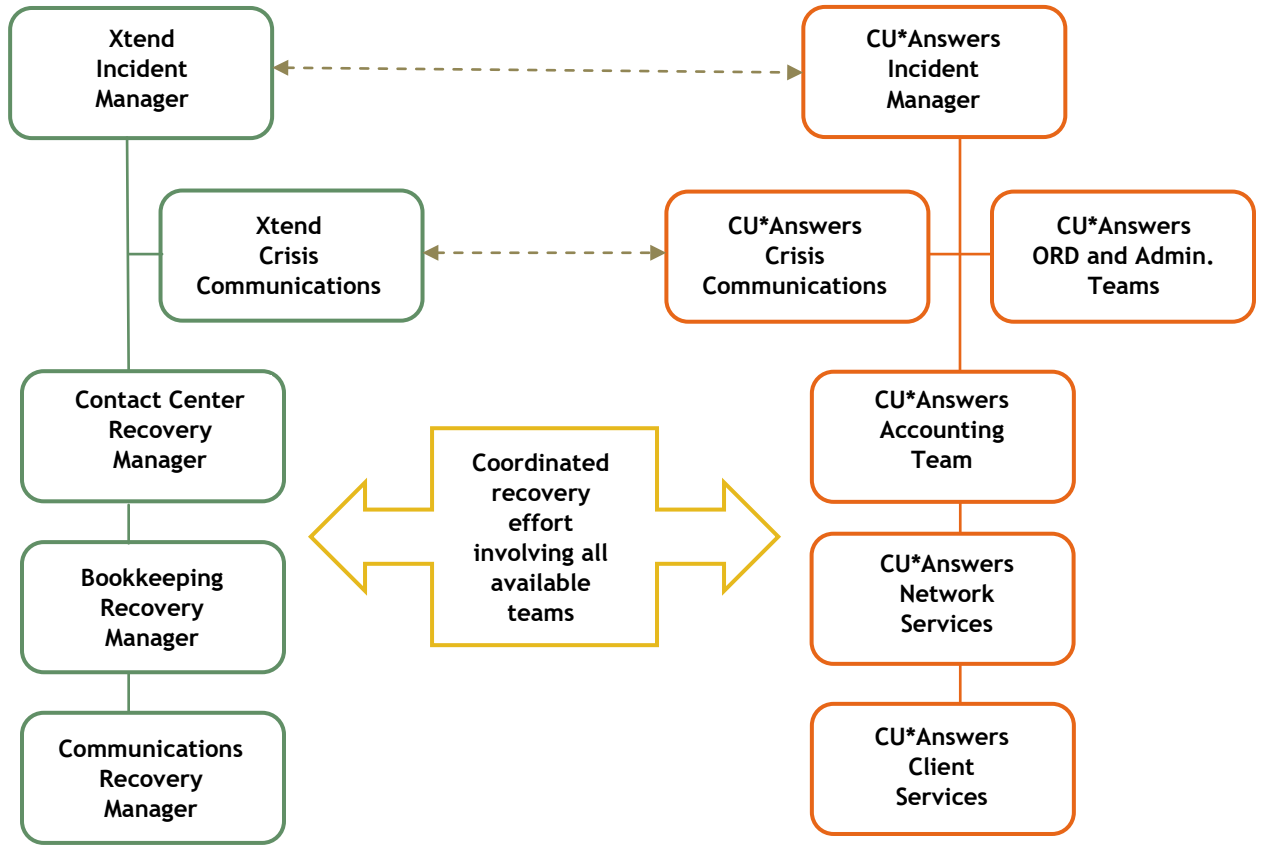
13. **Assessment of response and recovery efforts**
    a. Schedule debriefing meeting to evaluate the effectiveness of the disaster response.
    b. Identify required modifications for Recovery Plan.
    c. Prepare gap analysis report based on findings.

Roles and Responsibilities

An effective and efficient recovery requires skilled and trained personnel who are aware of their roles and responsibilities. The diagram and tables below show the Xtend and CU*Answers Recovery Teams and responsibilities of each. The Incident Manager has the authority to make changes as needed based on the circumstances of the event.

Perhaps the most important factor to ensure timely recovery is the quality and frequency of communication between recovery teams and management. It is critical that information is fed upstream to keep the decision-making team up to date on the status of the recovery efforts.

Staff emergency contact information is available in the "Appendix" section.



The following pages you will find specific responsibilities for each recovery team identified above. Each incident or crisis has its own unique set of circumstances and may require individuals and teams to perform multiple roles. It is important that each team is knowledgeable and trained to perform these and other tasks assigned to ensure a timely recovery.

Incident Manager	Responsibilities
✪ **President/CEO** CU*Answers as needed (Incident Manager)	• Oversee efforts of all resumption teams and ensure that recovery goals and timelines are met • Establish command/control center for management of incident • Primary decision maker on the invocation of the Emergency Response and Recovery plans • Serve as liaison to the Board of Directors • Communicate with recovery teams to inform them of strategic direction and the status of the recovery efforts • Resolve issues of priority based on evolving circumstances • Determine message communicated to external media • Oversee initial damage assessment and approve major equipment purchases • Offer guidance to local authorities, utilities, services, etc. • Locate and confirm alternate site selection and availability • Oversee, review, and approve any facility's renovation and construction • Inform and update Senior Management Team on recovery status

Crisis Communications	Responsibilities
✪ **Vice President of Communications** *CU*Answers as needed (Writing Team)*	• Serve as communications point of contact for the entire organization with external media relations (TV, print, web, etc.), public affairs, etc. • Serve as a conduit for all internal communications to and from executive and technical teams, alert staff, clients, major vendors, etc. • Message content creation and distribution (official company holding statements to minimize adverse publicity) • Organize internal meetings/briefings on recovery status (distribute recovery plans as needed) • Inform and update Senior Management Team on recovery status • Assist CU*Answers HR and Administration Teams in communications with personnel and families

Department Recovery	Responsibilities
✪ **Contact Center Management** ✪ **Bookkeeping Management** ✪ **Communications Team Management** ✪ **Administration Team Management**	• Assess scope of disruption and the impact specific to your department's operations • Identify critical functions based on the circumstances of the disruption • Inventory which resources are available and what is needed • Communicate status to Incident Manager • Mobilize team to available recovery workspace • Assist other recovery teams as instructed by Incident Manager • See "Department Relocation/Mobilization" • Inform and update Senior Management Team on recovery status

HR/Administration	Responsibilities
✪ **CU*Answers & Xtend (HR and Administration Teams)**	• Arrange travel, lodging, meals, and miscellaneous purchases for recovery staff as needed • Ensure proper office working environment for recovery staff at all facilities • Ensure injured/ill personnel receive prompt medical attention, families notified, etc. • Ensure all personnel/family issues are resolved (attendance, payroll, insurance/benefits, legal, etc.) • Answer questions about payroll continuation, employment, or securing temporary personnel during the recovery operation • Ensure workers compensation claims are properly filed and processed • Verify hours worked for staff and schedule sufficient time off • Hire temporary personnel as required • Inform and update Executive Team on recovery status

Accounting	Responsibilities
✪ **CU*Answers (Accounting Team) (Logistics Team)**	• Ensure adequate cash flow for expenses during recovery • Contact supply vendors to increase credit limits and expedite shipping due to nature of event • Establish emergency accounting and purchasing procedures • Aid in all monetary details associated with the recovery operations, recording of expenses, post recovery cleanup, intermediate emergency credit arrangements, petty cash, travel advances, etc. • Act as liaison with insurance agency to document, file and settle claims Inform and update Executive Team • Purchase, receive, store, distribute all software, equipment, and supplies, etc. • Maintain interface with supply channel vendors • Establish mail services area to handle mail for recovery personnel and express-shipping functions at all locations • Verify and maintain all receipts and paperwork • Inform and update Executive Team on recovery status

Network Recovery	Responsibilities
✪ **CU*Answers (Network Services Team)**	• Recover network infrastructure (LAN/WAN, etc.) including data and voice communications • Ensure network/data security and availability • Order, install, and configure networking equipment as needed • Confirm recovery-site data-communications lines specifications • Recover archived data environment and restore data from media for server and application recovery • Ensure the archiving of data during recovery efforts to protect against loss in disruption reoccurrence • Recover/restore servers and appliances for critical business applications and services • Inventory damaged and undamaged items, determine salvageable status of equipment • Identify and inventory damaged or destroyed equipment for insurance and replacement purposes • Repair, replace, install, configure all internal network user hardware (workstations, printers, etc.) • Make repair/replacement recommendations • Mitigate damage to remaining equipment and facilities • Oversee cleanup and restoration of damaged equipment and supplies • Coordinate ordering/receipt of replace • Organize the transportation of supplies, data, equipment, and personnel • Assist in establishing/preparing temporary facilities during recovery efforts • Coordinate movement and storage of salvageable items • Inform and update executive team on recovery status

Emergency Response Plan

Initial response to a (potential) incident is key to an effective recovery.

No document can contain all of the practical responses for the wide variety of circumstances related to all potential incidents. The emergency response Plan provides critical information and a prioritized list of procedures to be performed for a variety of scenarios with the common goals of:

- Safety of personnel (staff and guests)
- Security of data
- Protection of assets

The "**Emergency Response Team**" is a group of people who are prepared for and respond to any emergency incident, such as a fire and explosion or an interruption of business operations. An accurate and prompt Initial assessment and response during the first few minutes are critical to minimize impact and injury.

A disaster may be declared, and this Plan activated by the Incident Manager of any member of the Emergency Response Team.

For building service outages (power, communications, etc.) contact:

Melissa Medley at [CONFIDENTIAL]**or Dennis Richardson at** [CONFIDENTIAL]

Emergency Response Team

Name	Position	Cell Phone	Alt. Phone	Recovery Role
Liz Winninger	CEO	[CONFIDENTIAL]		Incident Manager/Crisis Communications
Nathan VanPatten	Manager of Contact Center	[CONFIDENTIAL]		Contact Center Recovery
Danielle O'Connor	VP of Accounting	[CONFIDENTIAL]		Bookkeeping Recovery
Jalyn Lindeman	VP of Communications	[CONFIDENTIAL]		Communications Services Recovery
Melissa Medley	Administration Manager	[CONFIDENTIAL]		Administration & Facilities Recovery

*See "Appendix" for staff emergency contact information

CU*Answers Emergency Contact Information

Name	Position	Cell Phone	Alt. Phone	Recovery Role
Geoff Johnson	CEO	[CONFIDENTIAL]		Incident Manager
Bob Frizzle	CFO	[CONFIDENTIAL]	[CONFIDENTIAL]	Business Recovery
Dave Wordhouse	EVP of Technology	[CONFIDENTIAL]	[CONFIDENTIAL]	IT Recovery
Heather French	VP Client Inter.	[CONFIDENTIAL]		Client Services Recovery
Scott Collins	EVP	[CONFIDENTIAL]	[CONFIDENTIAL]	Sales and Marketing
Chris Shelton	Network Services	[CONFIDENTIAL]		Network Recovery
Jim Lawrence	VP DR/BR	[CONFIDENTIAL]		Business Continuity/Operations Recovery

***See "Appendix" for staff emergency contact information**

Responsibilities of Emergency Response Team include (or delegation of):

- Identify the disruption.
- Assess the damage (facilities, equipment, services, etc.).
- Decide whether a disaster is to be declared.
- Alert recovery teams (keep track of mobilized personnel).
- Locate and confirm alternate site selection and availability.
- Adapt the Plan to account for prevailing circumstances.
- Prioritize recovery steps.
- Initiate, control, and coordinate recovery operations.
- Initiate communications with internal and external stakeholders.
- Approve expenditures related to the recovery process.
- Procure the replacement of destroyed or damaged equipment.
- Offer guidance to local authorities, utilities, services, etc.
- Review critical milestones during the recovery process.
- Document and log events as they occur.
- Provide recovery status information to management and board of directors.
- Assemble and verify information for the Crisis Communications Team, who will control its release to stakeholders.

Establishing Command and Control

Most incidents are relatively small in impact and have a short duration period. For example, a power outage, though somewhat frequent in occurrence (once or twice each year) is short lived (90% less than one hour) with an impact that has been dampened with the deployment of controls such as redundant power sources (UPS and generator). Other incidents can have a much greater impact but may be less frequent (building fire or explosion) however, they still require immediate action to limit and prevent injury and damages. With each incident, our response may be different, but the priorities are still the same.

Priorities:

1. Safety of personnel (staff and guests)
2. Security of data
3. Protection of assets

Once an incident is detected, it is important to establish command and control early in the recovery effort. Normal reaction may be that of confusion and chaos in an emergency situation. Therefore, coordination of personnel and resources during emergencies is a critical function of the **Emergency Response Team**.

The Emergency Response Team will establish a Command Center upon declaration of a disaster event. Alternative locations to the main office include space at CU*Answers' 28th street facility or a building equipped to accommodate the recovery efforts. The location will be disseminated to staff via established call tree processes and as specified in the Crisis Communications section.

Typical items necessary at a Command Center may include:

- Office supplies (pens, paper, paperclips, envelopes, files, folders, staplers, etc.)
- Fax/printer/copier (with supplies – paper/toner)
- Folding tables and chairs
- Whiteboard and dry-erase markers
- Check stock and specialized forms

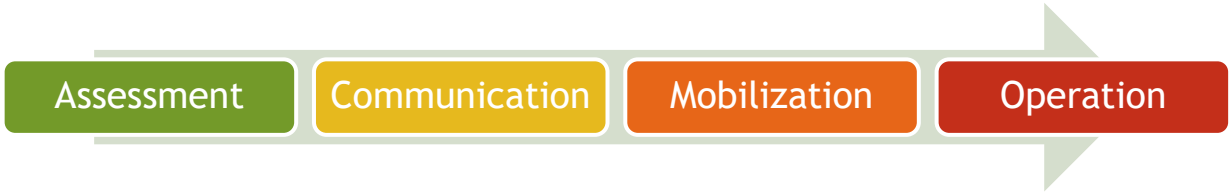
Emergency Response Checklist

- □ Conduct initial status meeting with Recovery Team leaders.

- ☐ Determine the extent of response and recovery actions to be performed.
- ☐ Establish frequency of communications to provide support and on-going status of current response and recovery activities.
- ☐ Observe all staff behaviors and as needed provide periods of rest and relief to relieve stress and correct inappropriate behavior.
- ☐ Maintain a log of recovery activities (problems encountered, suggestions for improvements to the plan) of each business function affected.
- ☐ Conduct an initial assessment.
- ☐ Determine the status of the work in progress at the time of the disruption and provide a status update to the stakeholders and management.
- ☐ Perform damage assessment.
- ☐ Determine criticality of damaged/destroyed items or components (salvage).
- ☐ Cell phone cameras can be used to document disaster area damage.

Department Relocation/Mobilization

The following example checklist has been provided for recovery team leaders to use as a guide during incidents where department relocation and mobilization is required.



Phase I: ASSESSMENT

- Receive initial disaster alert and instructions.
- Assess scope of disaster and what it means to my department (which services not available, expected duration, etc.).
- Activate department recovery plan as needed.
- Inventory which resources are available and what is needed.
- Identify obligations for assisting in the organizational-level recovery.
- Communicate to Business Recovery Manager what resources are needed and when.

Phase II: COMMUNICATION

- Notify team members of the situation.
- Verify who is available for work and when.
- Communicate if current staffing levels are adequate for recovery and operations.
- Request additional staffing if necessary.
- Re-assign unused personnel to assist in the organization-level recovery.
- Provide instructions for reporting to work (who, what, where, when).
- Provide any requests to the Administration Team for any transportation, lodging and food needs.
- Provide any requests to the HR Team for any personnel related needs.
- Coordinate with Crisis Communications Team for any external stakeholders (vendors, clients) who need to be contacted.

Phase III: MOBILIZATION

- Report to alternate location and assess the workspace recovery area.
- Establish communications methods between team members and frequency.

- Provide instructions for prioritized department recovery to each team member.
- Establish a staff schedule rotation at the alternate location during the recovery process.
- Coordinate the delivery and setup of required resources (equipment, supplies, etc.).
- Document problems encountered and corrective actions taken.
- Maintain records and receipts of all recovery related costs and expenses.
- Monitor and log the recovery process (or delegate).
- Communicate status to Business Recovery Manager (periodically as directed).

Phase IV: OPERATION

- Perform interim operation procedures (critical functions) at temporary location.
- Establish a staff Incident Manager (periodically as directed).
- Prepare for relocation to permanent location once available.
- Document problems encountered and corrective actions taken.

Declaration of Disaster

For incidents where long-term outages and high impact are expected, engaging, and mobilizing recovery teams and invoking the proper recovery plan quickly is imperative. This decision is most likely performed by the Incident Manager or member of the Senior Management Team.

Continuity Insurance

Insurance allows for the organization to recover losses that cannot be completely prevented, and expenses related to recovering from a disaster. Insurance coverage is obtained for risks that cannot be entirely controlled yet represent a potential for financial loss or other disastrous consequences.

Evaluation of Insurance Options

To offset potential losses, Xtend have purchased insurance coverage for identified perils. This coverage is referred to as business-interruption or additional-expense insurance. Exposures not addressed by insurance will be taken into account in the Business Recovery Plan.

There are two basic types of insurance: property coverage and time-element coverage. Property coverage covers buildings, personal property, and equipment and machinery. Time-element coverage covers such items as business income, extra expenses, leasehold interest, and rental value. CU*Answers maintains both types of insurance coverage.

Covered Perils:

- Explosions
- Fire or lightning
- Leakage
- Mine subsidence
- Riot or civil commotion
- Sinkhole or collapse
- Smoke
- Vandalism
- Volcanic action
- Wind or hail

Extensions to Normal Coverage:

- Electrical arcing
- Falling objects

- Glass breakage
- Mechanical breakdown
- Steam explosion
- Water damage
- Weight of ice, snow, or sleet

Property Coverage:

The value of insured assets is generally determined by a combination of methods including actual cash value, replacement-cost value, functional-replacement value, and book value.

Time Element Coverage:

The expenses incurred during the recovery of critical functions. Examples include business income -the loss suffered because we cannot provide our services.

Extra Expenses:

Coverage for those expenses that are beyond the normal operating expenses required to continue operations when premises are damaged during an interruption. The damage must be caused by an insured peril. Examples include:

- Disaster-declaration fees
- Rent for alternative office site
- Rent for fixtures, machinery, and equipment
- Light, heat, and power at temporary locations
- Insurance at temporary locations
- Moving and hauling
- Installation of operation at temporary location
- Employee expenses
- Administrative expenses
- Emergency command-post expenses
- Operating expenses

Insurance Agency:

[CONFIDENTIAL]

Emergency Response Procedures

Response procedures are identified below for the following scenarios:

- Fire/Explosion (requiring building evacuation)
- Severe Weather (requiring seeking safe shelter)
- Flood and Water Damage
- Power Outage
- Injury/Illness/Mass Absence (Pandemic)

Fire/Explosion

When a potential crisis is identified that requires the evacuation of building occupants for safety reasons, all persons should exit the building and at the designated assembly area. This is a safe distance from the premises and out of the way of arriving emergency services. When evacuating the building, all occupants should attempt to perform each of the procedures listed below providing it does not increase risk of injury:

Building Evacuation Procedures:

1. If you see a fire and/or smell smoke, report it to a manager immediately.
2. Engage the fire alarm if the situation warrants to alert others in the building.
3. If you are at your workstation and time permits, quickly grab your laptop and personal items (jacket, purse, cell phone).
4. Begin the evacuation process using the closest escape route. If route is blocked, use an alternate route.
5. Assist guests and others who are experiencing difficulty evacuating the building.
6. Report to the assigned assembly area and check in with your manager (or supervisor).
    a. Designated assembly areas include:
        i. Northeast corner of parking lot; near stairs to the CU*Answers parking lot
7. Provide any information you can of issues noticed during the evacuation or of persons still in the building.
8. Remain out of the way of emergency rescue personnel.
9. Do not re-enter the building until the “all clear” has been issued by the Evacuation Marshal (CEO or acting Marshal).
    a. Silencing the alarm does not mean the emergency is over.

Building Evacuation procedures are included in REACH education classes and a copy is available on Nucleus for all staff. Evacuation drills are to be exercised on an annual basis.

Purpose of evacuation drills:

The purpose of the evacuation drill is to:

- Educate the building occupants on emergency evacuation procedures.
- Assist in the evaluation of emergency plans (strategy, communications, etc.); and

- Identify potential issues with the means of egress.

Familiarity increases the probability of a successful evacuation during an actual emergency.

What you need to know:

Fire is always unexpected. A fire typically takes about 90 seconds to establish itself as a serious danger. Within five minutes it can get out of control. Quick response is required by a trained staff. A fire suppression system has been installed to detect and suppress fires (slow the spread) and alert occupants. Many minor fires can be put out with the prompt use of a fire extinguisher.

- Know how to detect and report a fire to alert others in the building.
- Remain calm. A disorganized evacuation can lead to confusion, injury, and property damage.
- Reporting to your supervisor at the proper assembly areas helps eliminate the need for dangerous search and rescue missions.

Confusion and panic can settle in once it's learned that the emergency is real.

- Always have at least two escape routes in mind in case the first one is blocked.
- Test doors for heat by placing the back of your hand on it (not the palm of your hand or fingers).
- Do not open a hot door. Seek an alternate escape route or take evasive actions such as crawling under a smoke layer in a corridor.
- Avoid using elevators when evacuating a burning building.

Roles and responsibilities:

In the event of an evacuation, everyone has an important role to play.

All Staff:

- Evacuate the premises in a calm and orderly fashion once the alarm sounds,
- Report to your department lead at the designated assembly area to make known your safety and whereabouts,
- Assist any guests that are with you,
- Report any issues to key personnel listed below, and
- Engage the use of fire extinguishers if required.

Assembly Area Coordinators: [Supervisors]

- Provide leadership at the assembly areas,
- Collect counts from Team Leads,
- Arrange for medical assistance for anyone in need,
- Report any missing personnel or other issues to the Evacuation Marshal, and
- Let CU*Answers know of evacuation.

Evacuation Marshal: [CEO or acting Marshal]

- Oversee the evacuation,
- Establish the chain of command,
- Communicate with outside emergency services,
- Provide leadership and direction for all staff,

- Engage the use of fire extinguishers if required, and
- Communicate “all clear” signal once granted by emergency services.

Assembly Area

[CONFIDENTIAL]

Severe Weather/Shelter-in-Place

Severe building damage and personal injury can occur during a severe weather event including:

- Lightning
- Tornado/high winds
- Snow/ice (dangerous driving conditions)
- Fog (dangerous driving conditions)

The top priority of the Emergency Response Plan is the safety of all personnel (staff and guests).

First aid kits are located in the employee break room at the Charlevoix location.

If a disruption to operations is foreseen, an alert should be posted for all clients and stakeholders (see “Crisis Communications” section).

Tornado/High Winds

If threatening winds (tornado, etc.) are present, all building occupants (staff and visitors) are to seek shelter in a location away from glass or other flying debris, preferably near the bottom of the building and windowless room, until an all clear is given.

No building occupant shall be permitted to leave the shelter area or the building until directed by management.

Lightning/Storm

If severe lightning is present, all personnel are encouraged to remain indoors and away from windows.

Hazardous Driving Conditions

If severe driving conditions are present (fog, snow, ice, etc.), personnel are encouraged to remain indoors until conditions improve.

Flood/Water Damage

Excess water and flooding can cause damage to multiple areas in the building, including the computer room. Repairs for structural damage can prevent staff from returning to their work areas. In severe cases, where large areas of flooring and drywall are in need of replacing, renovation can take up to 30 days or more.

Sources of water can include:

- Restroom (sink, toilet, water feeds, etc.)
- Kitchen (sink, dishwasher, etc.)
- Ceiling (water source and drainpipes, roof leaks, AC unit condensation leaks, etc.)
- Exterior doors, windows, and walls where water retention is possible
- Floor drains (failed sump pump)

- Fire rescue efforts (sprinkler system or fire hoses)

Damage can occur to:

- Electrical systems (building and computer room)
- Structure (weakening walls, floors, etc.)
- Paper documents
- Electronic media (tapes, hard drives, etc.)
- Computer hardware (i.e., corrosion)

In the event of flooding or other water damage:

- Determine if the Building Evacuation plan needs to be activated.
- Determine proximity/risk to computer room (power off equipment as necessary).
- Cover equipment with plastic tarps to protect from roof leaks (warning about humidity and corrosion on computer equipment).
- Determine source of water (roof, pipe, drain, wall, floor, etc.) and location of water-source shut off.

During the recovery efforts:

- Ensure that any hardware that is determined to be unsafe to operate is properly labeled. If determined to be safe, unplug equipment from the power source.
- Do not simply power equipment up until you are sure that that any moisture has been removed.
- Visually inspect equipment for external and internal damage. Do not power up any equipment prior to passing this inspection.
- Secure media in dry storage area.

Power Outage

What to do first:

1. Take a breath, relax, and think. Repeat this step before taking any action.
2. Someone from the management team should contact Consumers Energy to report power outage/determine restoration ETA. Communicate findings to the rest of the management team.

Staff should:

1. Come to work as usual if the outage occurs before work starts.
2. Report to their direct supervisor or manager for instructions.
3. Read Xtend's Power Interruption Response Plan thoroughly.
4. Stay away from areas where staff are handling the phones.
5. Refrain from adding extension cords and power strips to stations powered by the generator (power from the generator is not unlimited!).
6. Assuming the phones are working, use their personal phone to update their voicemail message and current status:
    a) 616.285.5711
    b) *
    c) 8 then their extension then their password then # (there won't be any prompts so just enter it all)
    d) 5 (for personal options)
7. Contact any clients with whom they have direct meetings/calls scheduled that day (see also Cancelling Special Events below).

8. Unplug any equipment vulnerable to damage from surges when the power comes back on.

Alerting clients:

Assuming web servers are up and that staff on the generator or using laptops is able to connect to the network**, wait at least 30 minutes** after the power goes out before posting an alert.

- Do not panic. Take a little time to determine whether it's a momentary glitch or a real outage.
- If the power goes off overnight, an alert should be posted between 7:00 and 8:00 a.m. ET. It is not necessary to send an alert in the middle of the night.
- Do not send an alert unless you have something to say.
- These people are responsible for posting an Alert to clients http://alerts.cubase.org
  - Writing Team (Andrew or Dawn)
  - QC (Pauline)
  - Ops (Todd or Jeff)

Cancelling special events:

If the power failure occurs on a day when a special event is scheduled where clients will be visiting our location, the team/person hosting that event should use the following questions to determine a course of action:

1. Have people already started to arrive or has the event already begun? Host should consider the unique situation and make a decision.
2. Is the power outage expected to last more than a couple of hours? If so, cancel the event.
3. Is there time to possibly stop travelers from leaving home? If so, contact attendees. Receptionists will have hard copies of attendee lists with emergency contact numbers printed as of 4 pm the day before.
4. Post an alert; mention that further communication will be sent once a reschedule date is determined.
5. After power is restored, the host is responsible for following up in order to reschedule and request the usual client communications from the Writing Team, etc.

Rules of thumb: Do not scramble around to try and move everyone to another site. Keep it simple and be mindful of cost. Relax and communicate that we're following our standard procedure for situations like this.

Working on building generator power:

All works areas (PCs, phones, etc.) are connected to the building generator and will continue to operate during a power failure (a reboot is required for those without battery backup). To ensure the generator will work when needed, a weekly inspection if performed by Xtend staff. The procedures are as follows:

Checking the Generator:

Frequency: Weekly

Process:

1. Grab the key from the Administration team.
2. Unlock the cage and door to the generator
3. Use up and down keys to navigate and record the running hours and number of starts
   a. Go to menu → Menu 4: Operational Records
   b. Use the down arrow to see total runtime
   c. Use the down arrow to see number of starts
4. Update the spreadsheet at: X:\Xtend\Management\Public\Administrative\Generator Maintenance

5. Send the update to Liz/Management

Tips for managers:

- Find out which other leaders are in the building or how they can be reached. Stay in touch with that person (for power restoration updates, etc.)
- Before you give permission to anyone on your team to use someone else's powered workstation or connect to the generator power, contact other key leaders in the building and coordinate priorities. You may need to negotiate based on demands on other teams.
- Flashlights are available at the main lobby reception desk.
- Make sure your team knows what you want them to do first. Should they call you? Wander into your office? Talk to their direct supervisor? Pack up immediately and go home? Pick an area for your team to congregate (away from people on the phones!); they should know to go there automatically.
- Do you have contact numbers for everyone on your team (and do they have yours)?
- Stay positive. A simple power outage is not a disaster, and for most teams it will be no different than a case in which someone calls in sick. Once you sort out and address the truly urgent tasks, meetings can usually be rescheduled, and priorities can be shifted. It is your responsibility to reassure your team and avoid unnecessary angst. You don't want to be the manager that overloads the generator or communicates the wrong message to a client because you overreacted.

Personnel Injury/Illness

In the event of injury to personnel (staff or guest):

- Determine if medical help is required.
- Ask for CPR qualified individuals if necessary.
- First aid supplies kits (including AED) are located in the employee breakroom, in a cabinet on the wall.
- Contact Human Resources who will contact family members if needed.
- Record identity of eyewitnesses and notes from event.

Instructions for Dialing 911

Remain calm and collected and:

- State "I have an emergency." (Wait for a reply.)
- State the type of emergency.
- State your name and number.
- State the exact location of the emergency.
- State if assistance is required (medical, fire, police, etc.).
- State the number of injured persons.
- State if a hazardous condition exists at the scene.
- State who is at the emergency scene.
- Wait for instructions before hanging up.

Large Scale Absence Policy (Pandemic)

(adopted from the CU*Answers Pandemic Policy)

This policy describes the procedures and controls implemented by Xtend to provide for continuation of business operations necessary to support our clients and partners should a large-scale absence impact our staff.

Policy Owner: Organizational Resource Development Team

Large Scale Absence Program

A large-scale absence, for purposes of this document, is defined by CU*Answers as missing 50% or more of the employee population for a period of up to 2 consecutive weeks. The determination that Xtend is experiencing a large-scale absence event will happen at the Corporate Officer level.

Method

Team leaders were asked to assess specific needs and concerns that they would face in a large-scale absence event for their area(s) within the company. These needs and concerns, the response or reaction to those concerns, and any preventative measures that can be taken have been used in the development of this planning document.

Client Services

Delays in servicing our clients should be expected. However, we would want to communicate this to the client appropriately by sending out a scripted message using our Alert procedures. Management must assist employees to prioritize the workload.

Coverage of all Shifts

Cross training and management involvement will help the client service areas to make sure all necessary shifts are covered across all areas of the company. Employees and managers who have the capability to work from home would be encouraged to do so if the situation allows.

Prioritizing Daily and Pending Duties

Time sensitive items must be considered. For example, if the timeframe is end of month, team members must be diverted across departments to complete important tasks. Management would make decisions on readjusting the priority list and delay of non-critical project travel.

Programming

The projects to be worked on will be prioritized by management; inevitably some projects will need to be delayed or put on hold for a short period of time. We will communicate this to the clients appropriately by sending out a scripted message using our Alert procedures.

Managing Project Timelines

Management will adjust these timelines and workloads (i.e., briefly delay new client launch, project delay, and demos if necessary.)

Responsibility for Resulting CU*BASE Issues

Cross training and updated documentation will be an important preventative measure to take in making sure a greater number of employees can be responsible for any CU*BASE issues. Employees and managers who have the access will be encouraged to work from home if the situation allows.

Delivering the Service to the Clients with Quality

For services that require travel, employees will be expected to be aware of their ability to complete their responsibilities without negative effects on the client. If necessary (i.e., in a conversion situation), Xtends' management may need to decide regarding whether more employees will need to be sent to supplement for the unavailable employees. For services delivered from our offices, cross-training and up to date documentation will be necessary to be able to continue to provide quality service. In some cases, CU*Answers and Xtend have relationship(s) with Staffing Agencies if additional staff is needed.

Handling Time-Essential Duties

Essential duties will still need to be completed; other team members will be assigned these tasks by management, as necessary. If possible, management will adjust these timelines and workloads by re-prioritizing duties.

At the Client Site

In a scenario where an entire team is unable to perform duties:

- Until additional staff can arrive on site, web and phone conferences would have to be utilized for training, support, sign-off etc. Several concurrent sessions could be scheduled to facilitate training by department.
- Depending on the location of the credit union, the CEO may tap other Xtend credit union employees as support staff.
- If the Credit Union is going through an event, the alternatives for signoffs, etc. are as follows: CPAs and Board members may be used as alternatives to a CEO for sign-off authorization; and
- Additional support may have to be rescheduled for a department, i.e., 'launch dates' may be postponed if several credit union employees are unavailable for the necessary training.

Shift Coverage and General Department Responsibilities

Adjust schedules of remaining team members to cover all shifts and run with reduced staff per shift. Managers will provide additional coverage as needed. Team members from other departments may .

Cross-Departmental Coverage Options

The call center & bookkeeping departments can also look outside of its own department in an event. Employees from other teams can be drawn upon to cover gaps in processing in the event of a serious shortage.

Communications

If Corporate Officers declare a large-scale absence event has occurred at Xtend, clients shall be notified via email Announcement and posted on the Alerts web page at http://alerts.cubase.org/alerts_for/xtend/.

Managers will be responsible for communicating to their staff members any new priorities or changes in responsibilities resulting from the event.

Travel During and Event

The travel expectations during an event will be decided upon by Xtend Senior Executive Team and communicated to the employees through HR. Depending on the circumstances surrounding the event, any decision could be made up to and including the suspension of ALL travel.

Additional Pandemic Policies

If the absence is due to a pandemic disease, the following additional controls are required: infected staff should defer coming to work for the length of the incubation period of the virus; staff should utilize the hand sanitizing stations provided around the office and wash hands often; clean keyboards and other equipment, especially if workstations are shared between staff members; a certain degree of social distancing could be practiced; reducing frequency, proximity, and duration of contact can also help reduce the spread.

Staff interactions during an event will be decided upon by Xtend Executive(s) and communicated to the employees through HR. Depending on the circumstances surrounding the event, decisions will be made regarding: severely discouraging or disallowing large assemblies of employees (on or off work premises); closing all meeting rooms; limiting all staff interactions as much as possible; encourage or force employees to work at home or at other CU*Answers offices; and/or offering masks and setting up for cleaning stations around the office.

Companion Documents:
Cleaning Protocols

Illness Reporting Protocols

Project Pandemic Response

All located here: X:\Xtend\COVID-19 DocumentsSecurity Incident Report

How to fill out a Security Incident Report

Submitting an Incident Report

Xtend CEO Incident Report

[CONFIDENTIAL]

[CONFIDENTIAL]

Distributed Denial of Service Attack Response (CU*Answers)

A number of critical products and services provided to Xtend clients require access to public-facing devices on the Internet that are exposed to the threats of a Distributed Denial of Service Attach (DDoS). These devices are hosted and provided by CU*Answers. For the purpose of this recovery plan, Xtend has provided the following:

*"**Distributed Denial of Service** attacks are just one type of threat faced by organizations that depend on the Internet for business transactions and communications. A description of DDoS attacks can be found in the CU*Answers April 2013 Whitepaper titled "Assessing DDoS Risk". In response to the heightened awareness surrounding the recent activity from these types of attacks, CU*Answers is providing this overview of the documented DDoS Incident Response Plan.*

PREPARATION

The best defense against such security attacks begins with a layered security strategy starting at each hardened host and expanding to security appliances at and beyond the network perimeter. Key to an effective incident response are the skilled and knowledgeable personnel that make up the Incident Response Team.

*The roles and responsibilities of the Incident Response Team are described in the "CU*Answers Incident Response Policy".*

COMMUNICATION

*A critical component of any incident response is timely, accurate and consistent communications at all points within the response phase to all internal and external stakeholders including senior management, affected clients and partners, legal counsel, vendors, and agencies including law enforcement (if appropriate). For use with all incidents and disruptions, CU*Answers has deployed the CU*BASE Alerts Notification Site, (accessible to CU*BASE on-line and in-house clients only) for posting current alert status information in conjunction with broadcast alert email notifications. All affected non-client stakeholders will be contacted using methods identified in the "Crisis Communications" section of the "CU*Answers Business Continuity Plan".*

DETECTION

*Proper detection of potential incidents begins with 24x7 network and host monitoring from multiple presence points within the network. With these monitoring and alerting tools in place, IRT members are notified around the clock of potential incidents that may require prompt response. Personnel are trained and skilled to take immediate measures to identify the type and scope of the incident and to accurately assess the risk to the organization (particularly the security, integrity, and availability of data on the CU*Answers networks).*

MITIGATION

*Once an incident is detected, mobilized IRT members may determine that mitigating steps are required, ranging from the limiting of access to/from specific hosts and networks to the complete protection of assets by prohibiting all traffic to/from specific hosts and networks. The Incident Response Team has been granted the "Authority to Act" as described in the "CU*Answers Incident Response Policy". Depending on the circumstances of the attack, the Incident Response Team may engage the cooperation of upstream service providers and security vendors if necessary.*

REMEDIATION AND RECOVERY

Once it has been determined that the incident/attack has elapsed and/or the risk has been reduced, the Incident Response Team will reintroduce services to the network until all have been restored. At the conclusion of the response effort, post-attack procedures include the collection of logs and potential forensic evidence (if applicable) and documenting response and mitigation procedure gaps, weaknesses and lessons learned."

IT Recovery

Overview of IT Environment

Technology resources used by Xtend staff to provide products and services to clients are leased and managed by CU*Answers. These resources include:

- Workstations and laptops
- Printers and copiers
- Data and Voice networks
- Network and information security
- Email server and applications
- VoIP phones and voice services
- Hosted applications (It's Me 247, CU*BASE/GOLD, MS-Office, etc.)

CU*Answers Network Services has been contracted for support of the above.

They can be contacted at x266 or at helpdesk@cuanswers.com or at x132 during after-hours to reach the support technician on-call.

[NETWORK DIAGRAM CONFIDENIAL]

Loss of Data Communications

Access to the internal network and to clients is provided by CU*Answers through redundant communications lines. The diagram above shows both primary and secondary gigabit networks connecting the Grand Rapids location to the Kentwood location. Connectivity to the public Internet and to the private client network is available through redundant Internet VPN and MPLS data lines.

CU*Answers maintains redundant data communications at both the Kentwood and Site-Four locations. In the event that data communications are not available through the primary Kentwood location, connectivity is redirected through the secondary Site-Four location.

Loss of Telephone Service

For Contact Center operations, Xtend depends on voice communication services provided by CU*Answers through its Interactive Intelligence environment.

The Interaction Client (I3) phone system is provided by servers at the 28th Street datacenter. Voice PRIs are brought into the datacenter on two circuits (one for local and another for long distance). Each circuit has a Cisco voice gateway appliance (redundant).

[NETWORK DIAGRAM CONFIDENIAL]

All system and network maintenance for the phone system is performed off-hours. In the event of a disruption of service, there is currently no alternate phone system configured. An alert (email/web) should be posted (see "Crisis Communication" section) to all clients and stakeholders. In the event of a long-term outage, instructions could be provided to contact one of the analog lines still available or a staff member's cell phone.

The following systems may be affected by an I3 phone system service outage:

- Xtend Contact Center, Collections, other campaigns
- Incoming faxes to DID #s
- CU*Talk
- Outgoing calls
- Incoming calls

Probable causes of service outages include:

- Call routing at carrier
- Physical line damage (back-hoe, groundhog, laying sidewalk, etc.)
- VoIP GW hardware/software failure
- CIC server hardware/software failure
- LAN switch-stack failure
- Phone firmware upgrade

Internal I3 phone-system support personnel include:

[CONFIDENTIAL]

Local carrier: [CONFIDENTIAL]

Long Distance and Toll-free: [CONFIDENTIAL]

Xtend procedures to follow during phone outage:

In the event of a phone system outage, Xtend will coordinate with CU*Answers to alert all clients of the incident and expected duration of the outage.

*See "Crisis Communications" section on posting an alert.

Business Recovery

A disruption that imposes the relocation of staff and/or critical resources to another area within the facility or to an alternate/temporary facility can be the result of several scenarios such as:

- Loss of service (HVAC, communications, power) is expected to last several days
- Loss of access or physical damage to the structure (fire, water, flying debris, other)
- Large-scale renovation project (planned)
- Hazardous material spill (quarantine)

Recovery steps include:

- Conducting an initial assessment of outage to determine the duration and scope of the event and business functions to resume
- Identifying alternate facilities and arranging for operations
- Notifying employees and providing instructions on where to report and when
- Determining if alternate skilled staff is required for the recovery effort
- Swinging communications to an alternate site (if needed)
- Retrieving records, supplies and resources required to resume operations from off-site
- Determining the impact of the work in process at the time of the disaster
- Determining materials needed (Office and IT equipment)
- Approving and arranging for purchases
- Setting up shipping/receiving operations for the facility (UPS, FedEx, USPS, etc.)
- Ensuring security of assets and safety of staff at each location (physical access, video surveillance, lighted parking lot, etc.)
- Coordinating the repair and restoration of the disaster site

Office workspace recovery options include:

- Relocating to an alternate space/floor within the same building (if damage is contained to small area and access to building granted)
- Working remotely from home, a hotel, or a conference room (assuming SSLVPN access is available)
- Leasing equipped work-recovery-area services (dedicated, shared, mobile)
- Working from available space at a CU*Answers' office location
- Securing available commercial space from landlord

Office workspace recovery requirements include:

- Workstations (monitor, mouse, keyboard, scanners)
- Power distribution units, lighting
- Desk, table, chair
- Printer, copier, fax, shredder, phone
- LAN, switch, cables
- Paper, envelopes, blank checks
- Extra cell phone chargers
- Whiteboard, markers, easel, flipcharts
- Pens, pencils, staplers, paperclips

In the event of a large-scale relocation effort, Xtend will coordinate with CU*Answers for the recovery and resumption of critical business functions.

Xtend Business Units and Critical Functions

The scale used categorize business functions is shown below:

- **< 4 hours**: Clients need and expect us to be able to provide this with minimal downtime. Very important.
- **< 8 hours**: Clients can operate but would feel the impact if downtime exceeds 8 hours. Still important.
- **< 24 hours**: Clients can operate and close the day but expect us to be back by the next day. Somewhat important.
- **48-72 hours**: Clients are inconvenienced but not significantly impacted. Not as important.
- **72+ hours**: Clients benefit from this but are not impacted during downtime. Non-essential.

Xtend Bookkeeping (minimum staff 4) Business Unit Lead: Danielle O'Connor

Critical Functions	Recovery Time Objectives
Bill Pay	< 4 hours
EOM Processing	< 8 hours
Work Daily Exceptions	< 4 hours
Daily Balancing	< 8 hours
Daily Posting	< 8 hours

Xtend Communications (minimum staff 1) Business Unit Lead: Jalyn Lindeman

Critical Functions	Recovery Time Objectives
HTML eStatement Notifications	< 8 hours
Lockbox Processing	< 24 hours
eNewsletter Service	48-72 hours
Member Reach	< 24 hours
Online Banking Banner Ads (Manage content library and delivery services)	72+ hours
RevGen	< 24 hours

Xtend Contact Center (minimum staff 4) Business Unit Lead: Nathan VanPutten

Critical Functions	Recovery Time Objectives
Provide Phone Support for Credit Union Members	< 24 hours
Web Chat	< 24 hours
Handle Inbound/Outbound Call Campaigns	< 24 hours

Crisis Communications

In a crisis situation, communication can make or break a complex recovery effort. It is important that internal stakeholders are informed of the situation and know what is expected of them (where to report and when) and that external stakeholders are made aware of the (potential) disruption to business functions and services.

Crisis communications must begin early in the recovery process beginning with notification of recovery teams and continue through the event until business has returned to normal.

Communications to external stakeholders during a crisis situation is best performed by a trained and/or experienced media spokesperson.

With effective crisis communications:

- Employees feel reassured
- Stakeholders feel confident in the response
- Media reports are accurate

Communications in a crisis is all about who, what, when and how.

- Who?
  - Staff (and their families), board of directors, members, vendors, service providers, emergency personnel, media, local/state/federal agencies, etc.
- What?
  - A carefully constructed message that generates confidence and assurance
- When?
  - Timing and frequency of the message throughout the disruption
- How?
  - Which communications channel to use for each group (email, phone, fax, web, etc.)

Key Stakeholders

Circumstances with each crisis scenario will determine who needs to be contacted and when. Stakeholders can be categorized as internal and external, each requiring unique message content.

Key stakeholders include:

- Internal audiences such as
  - Employees, and family members
  - Corporate management
- External audiences such as
  - Credit union members
  - Vendors
  - Partners
  - Regulators
  - Media including
    - Print
    - TV
    - Radio
    - Web

To internal stakeholders consider stating:

- Facts about the situation
- The response initiated by management
- Ways employees can report to their managers
- Employee assistance programs offered

- How the event might affect operations over subsequent days

To external stakeholders consider stating:

- Facts about the situation
- What Xtend is doing to resolve the incident and what each stakeholder can expect as a result of the incident (how it may affect them)
- Expected duration of the event
- Open issues that management continues to investigate

Communicating in a Crisis

All questions from the news media or others regarding the Plan or any disaster should be directed to the Incident Manager or CEO.

Methods of communication include:

- Email (corporate or personal)
- Instant messaging or phone texting
- Xtend corporate web site
- Social media tools such as Facebook, Twitter, LinkedIn, Skype, WebEx, etc.
- Phone (voice)
- Press conference
- Press release (print)
- Fax

Creating holding statements, which are pre-written statements for use in a variety of crises such as natural disaster, fire, explosion, public health emergency, and workplace violence incident, helps ensure that all relevant information is provided quickly and accurately.

Holding statements should identify the primary audience, the optimal delivery time, suggested method of delivery, as well as who should/should not deliver the message. Also, expect and be prepared for follow-up questions.

Key points to remember during and after the incident

- Remind employees that only media-trained personnel should speak to the media.
- Weigh the desire for information against the need to issue a statement.
- You will not know everything immediately.
- Give them what they need to know in the most appropriate method possible.
- Update the status often, even if there is no material development. This helps those connected feel they are in the loop on key details.
- Keep the information fresh and frequent (minimize waiting time between comments).
- Realize that the media is one of your best resources.

Publishing Alerts

Rev. August, 2021

This document outlines the basic steps for requesting an Alert to be published on the client Alerts website.

Procedure for Requesting a CU*BASE Alert

DO NOT JUST SEND AN EMAIL!!!! You must actually speak to the person on the phone or in person. By the time an email is read, it may be too late to publish an alert!

CALL OR VISIT the first person on the publish list below. If they are unavailable, contact the second person, then the third person, and so on. Do NOT contact all of them at the same time or multiple alerts might be published.

Procedure for Requesting an Xtend Shared Branch Alert

If the alert is urgent, use the same procedure as for a CU*BASE alert, but in general these are not urgent. Send an email to the first person in the publisher list.

Who Can Publish?

The following people have the ability to create alerts and are listed in the order in which they should be contacted when an alert is needed.

CU*Answers Publishers

[LIST CONFIDENTIAL]

Notice there aren't email addresses listed here. That's because you're supposed to CALL or VISIT them!

Others to contact if needed (also see "need help writing content?" on the next page):

**People who can help with WordPress software issues*

[LIST CONFIDENTIAL]

Special Note about After-Hours (Operations) Alerts

If alerts are needed early in the morning or after normal working hours, then the three names in Operations move up to 1st and 2nd position on the list.

Instructions for Publishers

Rules for Publishing Alerts

Alerts are designed for quick communications about urgent matters, particularly ones that won't live for a long time. Things like **It's Me 247** or CU*TALK being down, a data integrity issue found in the software, errors we are working on right now or anything with a relatively quick ETA.

If the problem will likely be resolved more quickly than it will take to create the alert (send it out, clients receive their emails and read them, etc.), an Alert may not even be created. That should be a judgment call on the part of the publisher and the programmers or other parties involved.

Need help writing the content of an alert? Contact someone on this list for help:

[LIST CONFIDENTIAL]

Sometimes an actual email would be better:

- If the communication isn't urgent
- If the information will need to be referred to again (such as a schedule of upcoming HA rollovers)
- If the communication is "official" and would maybe need to be communicated to a Board or printed and put into a file (such as a security breach)

In cases like this you can still publish an alert, but also do a normal announcement that can be emailed and posted on the News or other page of the website for later reference.

Library of Common Alerts

Go to the Portal > CU*Answers > Responding to Emergencies and look just below the publisher list for a list of common alerts. Just copy and paste this content into your alert, adjusting it as needed for the particular situation.

Tips for using the Alert Software

The Alerts site is available to all CU*BASE clients via the option on the Net drop-down menu in CU*BASE GOLD.
For those authorized to publish, here are some tips:

[CONFIDENTIAL]

Sending the Alert Email

After an alert is published, an email must be sent manually to the broadcast email list (email groups are in an Outlook public folder). The only difference between these is the ATTENTION line and the URL, so you can combine them or change them up as needed. **Remember that self-processors sometimes get alerts that online CUs don't and vice versa!** Regarding the Xtend email, you will only send one email, not two, to all online and self-processors (one email because the link is the same – to the Xtend Alerts page).

Refer to the separate "Announcing Something to Clients" document for hints on setting up your Outlook and addressing the email itself to all clients.

→For text you can copy, look below the pictures.

Sample Email to Online Clients
[IMAGE CONFIDENTIAL]

Sample Email to Self-Processors
[IMAGE CONFIDENTIAL]

If the alert only pertains to online or self-processors, adjust this attention line accordingly

Direct Link to the alert that is being referenced

Choosing the Email Addresses when Sending the Alert Email

1. Click BCC (might have to display this field, if you don't already Options tab on the ribbon)
2. In the Address Book drop-down, choose "Client Online" or "Client Self Processor"
    a. *TIP: See below for instructions on if you don't see this in the list*
3. Click on the first CU name in the list
4. Hold the **Shift** key and tap the **End** key
5. Press Enter or click the BCC button at the bottom of the list

Text you can copy to an email:

Subject Line = CU*BASE Alert: xxxxxx

ATTENTION ONLINE AND SELF PROCESSING CREDIT UNIONS

An alert has just been posted on the **CU*BASE Alerts!** page. **Read It Now**
To read all recent alerts, click the **Network Links** button on any CU*BASE GOLD screen and choose the **Alerts** link. (http://alerts.cubase.org/alerts_for/cuanswers-online/)

CU*ANSWERS | PLEASE DO NOT REPLY TO THIS MESSAGE | Refer inquiries to: AnswerBook

Subject Line = CU*BASE Alert: xxxxxx

ATTENTION ONLINE AND SELF PROCESSING CREDIT UNIONS

An alert has just been posted on the **CU*BASE Alerts!** page. **Read It Now**
To read all recent alerts, click the **Network Links** button on any CU*BASE GOLD screen and choose the **Alerts** link. (http://alerts.cubase.org/alerts_for/self-processor/)

Linking an Alert to an Email

It can help to have a direct link to the alert in question, to avoid any confusion on the part of our clients. When prepping an email to send out alongside the alert, be sure to copy the URL of the alert in question and link it to the email via the following steps:

- Click on the 'Insert' tab at the top of your Outlook email window, then highlight the 'Read it Now' text in the signature line of the alert email.
- Then, click on the 'Link' button near the top right of the Outlook email window. When a new window opens, paste the alert URL into the 'Address' line and select the 'OK' button.
- Test the link prior to sending by holding the 'CTRL' button and left-clicking with the mouse on the 'Read it Now' text.

Add Email Group to Outlook Address Book

In order to choose client names for the broadcast emails, you must first add both the online and self-processor list to your dropdown in Outlook, so it shows up here:

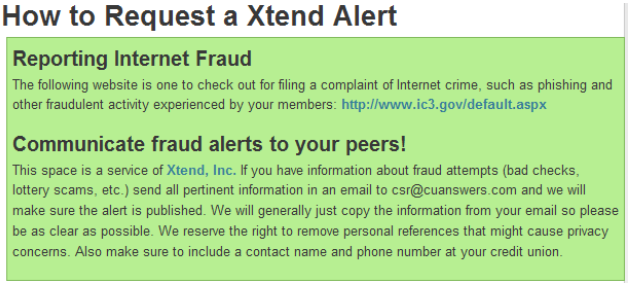
[IMAGE CONFIDENTIAL]

Rules for Xtend Shared Branch Alerts

Procedure for Requesting an Xtend Shared Branch Alert

If the alert is urgent, use the same procedure as for a CU*BASE Alert, but in general these are not urgent. Send an email to the first person in the publisher list.

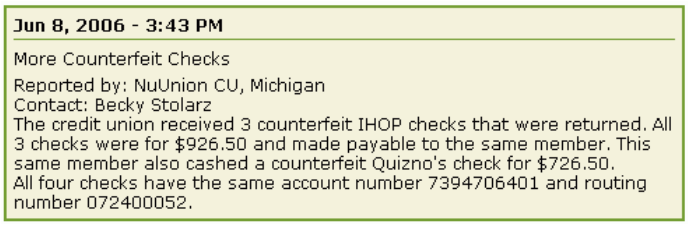
Here's what we tell clients to do on the site →



Xtend alerts are specifically in-network alerts that network participants are telling each other about something they personally know about regarding specific fraud attempts, bad checks being passed, etc. These types of alerts are not "I got this in my email, please pass it on" chain-mail communication. If a credit union has an article that they would like to pass along, they can contact Xtend Member Reach, who will call them with pricing, timing, etc. for the article they'd like to pass along. Additionally, you could ask Web Services if they would publish a story/article on cusecure.org as they are always looking for material for this security-geared website.

Since Xtend alerts typically come directly from clients, they usually need some wordsmithing. Keep in mind things like member privacy - just because a CU says a member is a bad guy, doesn't mean he really is (someone might even be using someone else's name). So, keep the amount of private info to a bare minimum and/or use verbiage like "a person claiming to be John Doe." Also, avoid any editorial comments like "we've had lots of trouble with this guy" or "yay, we caught him!" Just the facts, ma'am, just the facts.

Include a "Reported by" line with the credit union name and a "Contact" line with the person's name who reported it to us, as in this sample.



Regarding publishing the Xtend alert, the only difference is that you check the Xtend box and not the Online and Self-Processors boxes in WordPress.

Text you can copy to an email:

Subject Line = Fraud Alert: xxxxxx

ATTENTION ONLINE AND SELF-PROCESSING CREDIT UNIONS

A fraud alert has just been posted on the **CU*BASE Alerts** page. To read it, click the Network Links button on any CU*BASE GOLD screen and choose the Alerts link. (http://alerts.cuanswers.com/alerts_for/Xtend/)

Xtend | PLEASE DO NOT REPLY TO THIS MESSAGE | Refer inquiries to: info@xtendcu.com

Appendix

Xtend Staff Emergency Contact Information

(As of 10/17/2022)

Last Name	First Name	Ext.	Job Title	Alt. Phone	Cell Phone

[CONTCT INFORMATION CONFIDENTIAL]

Board of Directors

Board Member	Credit Union	Phone Number	Email Address

[CONTACT INFORMATION CONFIDENTIAL]

Vendors and Service Providers

In addition to vendors listed in the CU*Answers Business Continuity Plan

Vendor Name	Description	Phone Number	Email Address

[CONTACT INFORMATION CONFIDENTIAL]