WORKSHEET

Tackling the Target Breach

10 Tactics to Start Today

Trust is the cornerstone of a great member experience. In the wake of December's Target breach, credit unions are feeling uneasy. Some credit unions have chosen a proactive stance, reissuing cards for all members affected. Other credit unions have taken a wait-and-see approach, covering the fraud as it has occurred. Regardless of your risk management strategy, you can employ the following tactics to ensure that a breach of this caliber doesn't catch your members or your organization off-guard in the future.

- What have we learned?
- What will we prepare for in the future?
- What will we do differently?

In the sections below we discuss 10 tactics to help your credit union learn from the Target breach and prepare for the future, and how these tactics apply to each functional area in your organization. We recognize that every credit union is unique, so please apply these concepts to titles and departments as you define them. We urge you to share this information with your executive or management team, so everyone may better prepare in the future.

LEADERSHIP

CREATE A GUIDING COALITION: **Member security is of the highest priority.** This is an opportunity to demonstrate the importance of security at every level of the organization. Bring your team together and identify key stakeholders in the initiative. Empower them to make a difference, whether by identifying areas of concern or recommending new processes.

FINANCE

MANAGE RISK-BUDGET FOR FRAUD: Most credit unions have been discussing the cost of reissue and the potential cost of covering fraudulent charges. This breach has been expensive. In the future consider budgeting dollars for this extended member service. Base this line item on your fraud history, membership numbers, card holders, and proactive stance. Similar to an allowance for loan loss, this will make emergency funds available. Quite differently than the ALL, you control these dollars and they can be applied directly to the bottom line if deemed unnecessary for the year.

TECHNOLOGY AND ELECTRONIC SERVICES

EXAMINE YOUR STRATEGIC ALLIANCES: Debrief with the technology, electronic services, retail delivery and management staff to analyze the overall response and procedures, and follow up with strategic alliance partners/vendors. Determine the effectiveness of your Fraud Monitoring Center in regards to reaction time, anticipation of your needs and turnaround. Define what needs to be improved in the future and if there is a serious concern about reliability.

ENGAGE COMPLIANCE: Anticipate the regulator response. Are there regulatory issues you'll have to address or documentation that will be required based upon the impact to members or internal security? In addition, monitor Consumer Financial Protection Bureau alerts to ensure that your communication with members reflects their recommendations.

OPERATIONS, MARKETING AND EDUCATION

COMMUNICATE: Get employees engaged in the dialogue. Communicate powerfully and communicate often. In a situation such as this, internal communication can be more important than external communication. Many credit unions are doing an excellent job of delivering letters, reissuing cards, and extending services to their members. Don't forget to communicate extensively with your branches, call center, business development reps and anyone else in the trenches with your members. Rely on remote locations to tell you how members are affected in their areas. **It doesn't matter how well written your member communications are if your front line cannot articulate this message effectively.**

USE SOCIAL MEDIA: Social media is the perfect place to reinforce your member communications. You can post FAQs or lead people directly to your website for more information.

CROSS-SELL: Remember, cross-selling is merely educating your membership on your products and services. Why not educate members on the convenience of mobile banking and online banking? These services will help your members to be aware of their accounts on the go.

EXECUTIVE AND HUMAN RESOURCES

DOCUMENT YOUR PROTOCOL: Most of your data recovery and business resumption plans already contain information on disaster recovery, financial and otherwise. Use the content and procedures you followed with this breach as a template for future issues. Save member communications, cost analysis, and so on, so that in the future, managers immediately know the protocol for dealing with a breach.

ENGAGE HUMAN RESOURCES: The Target breach occurred at the worst time for staffing and scheduling. For many, managing a limited staff meant relying on personnel in different departments to help cover. In a crisis situation like this one, don't be afraid to pay overtime for employees who help to reissue, return member communications, and lend a helping hand.

REWARD THE STAFF: Reward the people who worked together to make a difference to members and collect stories that help you communicate internally the credit union difference.

Produced for CO-OP Financial Services by Dr. Brandi Stankovic, Partner at Mitchell Stankovic & Associates.

CO-OP Financial Services
9692 Haven Avenue
Rancho Cucamonga, CA 91730

CO-OPFS.ORG

CO-OP FINANCIAL SERVICES

Be There Be More

02032014CF1430