***NOTICE****: The following has been provided by WBA committee and section volunteers for use by member banks.
It should be reviewed and revised as appropriate to the user-bank’s own policies, procedures, and practices.*

**Data Breach Communication**

How do you respond to a data breach? Be proactive. Customers need to hear that your bank is working to protect their information. Bank staff members, especially frontline employees, need to hear from management what steps are being taken and how they can address customer concerns.

Contacting customers shows that the bank is proactive. You’re demonstrating through your actions that the bank is actively protecting its customers rather than waiting for fraud to occur. When communicating with customers after a data breach, try to anticipate their questions. Send a letter or secure email including a summary of what occurred during the breach, why the bank believes the customers’ information may be compromised, and exactly what the bank is doing to address the situation. Be as transparent as possible. Once you have a draft, read the letter over and come up with as many follow-up questions as possible. Rewrite the message to address those questions.

For example, if you are deactivating cards that have rewards associated with them, what happens to accumulated points associated with the card? If cards are not automatically deactivated, what should customers do if they want a new card anyway? Answer as many customer questions as you can in your initial communication.

However, you’ll never address every possible concern the first time. Once you start receiving customer questions about the letter or email, keep track of the most common ones. Use them to train frontline staff so they’re prepared for questions when customers call or come into the branch. If a large number of customers have the same question, consider sending a follow-up communication or even a phone call if it’s feasible logistically.

After a data breach, it’s also important for bank management to communicate with staff. In this communication, go into detail about how the bank is reacting to the breach, including which specific products and/or services will be affected by those actions. More importantly, explain why the bank is taking those actions. Knowing the reason behind what’s happening will help frontline staff explain the situation to confused customers. If there are any important talking points concerning the breach that staff should use when speaking to customers, be sure to highlight them in the email, letter, or staff meeting.

Finally, for both customers and staff, explain where they should go with additional questions or for more information. Remember, your main goal is to make customers feel their money is safe and ensure bank personnel are confident in addressing customer concerns.

**Talking Points, Themes, and Security Tips**

Listed below are a variety of potential themes and talking points for your bank if a data breach has occurred and is causing you to reissue cards. Be sure to tailor the most appropriate points to your specific situation. You should also check your company’s mission statement as there may be an opportunity to work that theme into your communications.

* Outline the steps the bank is taking to prevent further fraud. Include a summary of what has occurred and what additional steps the bank is taking.
* The bank’s first priority is to protect you, the customer, and rectify the situation if fraud affected your finances.
* Offer security tips to your customers. Those tips can include:
	+ Protect your home wireless network with a strong password of at least eight characters, including upper and lowercase letters, numbers, and special characters. Change passwords regularly.
	+ Keep your computers and mobile devices up to date with the latest security software, web browser, and operating system.
	+ Check your accounts frequently for suspicious activity.
	+ If you suspect fraud, contact your financial institution right away.
	+ Keep your receipts and check them against your statements.
	+ Keep a record of card numbers, expiration dates, and your bank’s phone number in a secure but handy place.
	+ Don’t leave bank statements, checkbooks, credit cards, or debit cards lying around the house or at work. Keep confidential information secured and protected.
	+ Don’t give out personal financial information to callers, or those who seek it in emails.
	+ If you suspect wrongdoing, contact the [Federal Trade Commission](https://www.ftc.gov/) (FTC) at
	1-877-438-4338 or write the FTC at the Consumer Response Center,
	600 Pennsylvania Avenue N.W., Washington, D.C. 20580.
	+ Obtain your credit reports from each of the three nationwide credit reporting agencies every 12 months. Look for incorrect information, which could be a sign of identity theft. Get started by going online to [AnnualCreditReport.com](https://www.annualcreditreport.com/index.action), or call
	1-877-322-8228.

**Actionable Items**

* Write and produce Q&As, facts sheets, letters, or emails for the following groups:
	+ Employees
	+ Customers
	+ Shareholders (if applicable)
	+ Website (a message from the president)
* Designate an official spokesperson (should be the president or CEO of the bank) for any potential media calls. The message must be delivered in a matter of fact, positive voice and attitude.
* Concentrate on your teller line.
	+ They need to be able to answer basic questions in a matter of fact, positive voice and attitude.
	+ They need to hand out pertinent materials to customers.
* Make sure senior staff are available for any customers that have questions or concerns. Instruct teller line to offer senior staff access to customers when appropriate.
* Set up Google Alerts to monitor news regarding the bank in case customers turn to the press. This should be set to search “everything” and “as-it-happens” in Google’s search parameters. All terms should be entered as shown below. Quotation marks and other symbols are part of Google’s search methodology. Depending on the name, you should also consider including common misspellings of your bank and president or CEO’s names. Terms should include but are not limited to:
	+ “Name of your bank”
	+ “Name of your president or CEO”
	+ “Wisconsin” + “bank”
	+ “Wisconsin bank”
	+ “Consent order”
* Respond to negative feedback with a single response. You should be monitoring:
	+ Letters to the editor
	+ Blogs
	+ Comments on newspaper online forums
	+ Social media