CUNA MUTUAL GROUP

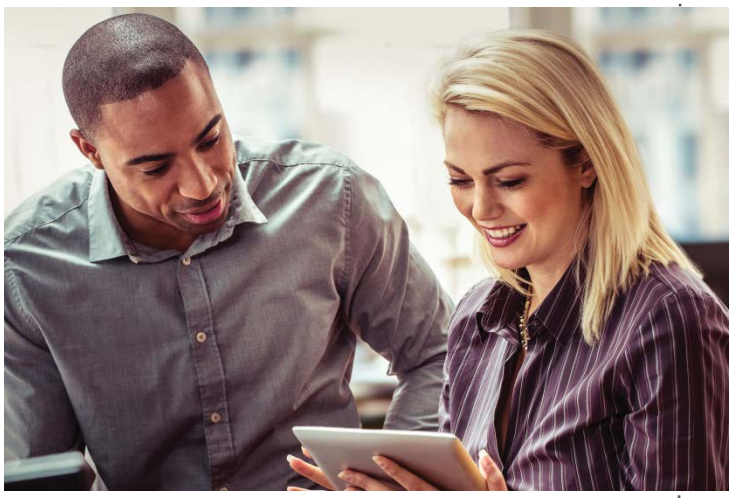
Post-Breach Consumer Tips

Minimizing member risk

#MemberTips

Data breaches pose a potential risk to consumers in the form of identity theft, account takeover, and fraud when personal and sensitive information is compromised.

Encourage your members to follow these tips following a breach that has exposed personal information. These tips are a good way to minimize the risk or impact of data breaches.



Helping members know what to do post-breach can minimize the impact of scams

Credit Reports

If any portion of your member's Social Security Number was compromised, the member should consider ordering a credit report and closely review it.

Encourage members to place a **security freeze** on his/her credit report. A security freeze, also referred to as credit freeze, protects the member by restricting access to the credit report. During a freeze, the credit union, along with other financial institutions or lenders, are blocked from ordering the member's credit report unless a pre-set PIN is provided to lift the freeze.

Members will have to allow for extra time for a loan or credit approval after placing a freeze. Members will have to request the security freeze from each credit bureau – Equifax, Experian, TransUnion, and Innovis.

In some states, the credit bureau charges a fee to freeze, temporarily thaw, and/or unfreeze a credit report.

Fraud Alerts

Place a fraud alert on the member's credit report if he/she is a victim of identity theft.

When a financial institution or lender pulls a credit report containing a fraud alert, they are required to call the phone number contained in the alert, or use other reasonable means to verify it was actually the member that applied for an account or loan.

An initial fraud alert remains on the member's credit report for 90 days and must be renewed while an extended fraud alert remains on the credit report for seven years. The member can contact one of the three major credit bureaus to have a fraud alert placed on his/her credit report and that credit bureau is required to notify the other two bureaus.

Military personnel on active duty can place an active duty alert on their credit report following the same process.

CHECKING CREDIT REPORTS

Consumers are entitled to a free credit report every 12 months from each of the major consumer reporting companies. Members can request a copy from **AnnualCreditReport.com.** The free credit report will show all lines of credit and other obligations, along with other public data. **Items to watch for are "new" or "re-opened" accounts and other suspicious activity.**

Risk & Compliance Solutions • 800.637.2676 • riskconsultant@cunamutual.com

Post-Breach Member Tips

Online Login or Password Information

If any of your member's online login or password information was compromised, you should instruct him/her to:

- Log in to the member account as soon as possible and change the login and password.
- Make changes to accounts that use the same logins and passwords for multiple sites.
- Always use strong passwords that are at least 11 characters in length that are case-sensitive and include alpha-numeric characters and at least one symbol.
- Use a password checker to ensure he/she has implemented a strong password.

Debit or Credit Card Information

If the member's debit or credit card information was compromised:

- Call the credit union and request the old card to be canceled and request a new one.
- Review account activity and report any unauthorized transactions on a timely basis.

Credit Union Account Information

If credit union account information for a member was compromised:

- Review account activity and report any unauthorized transactions.
- Consider closing the account and request a new one, but be mindful of potential delays and interruptions to any automatic payments or deductions.

Protect Members from Scams

- Be mindful of emails or phone requests claiming to be from the business or financial institution which was breached.

  Phishing emails often contain attachments or links to malicious websites infected with malware. Avoid opening attachments and clicking on links contained in emails received from unfamiliar sources.
- Be wary of SMiSHing attacks which are similar to phishing but in SMS text messages. Avoid clicking on links or calling the telephone number contained within text messages received from unfamiliar sources.
- To avoid tax identify fraud make a point of filing annual tax returns promptly.

  Should the member be notified that more than one return was filed in his/her name, owe additional tax, or that records indicate that earnings were more than the amount of wage reported, complete an IRS Identity Theft Affidavit form 14039, and contact the IRS Identity Protection Specialized Unit at 800.908.4490.
- Encourage members to check with the credit union for additional account protections such as security challenge pass-phrase, account notes, and travel protections.
- In general, members should be wary of offers that are too good to be true, require fast action, or instill a sense of fear.

Risk & Compliance Solutions • 800.637.2676 • riskconsultant@cunamutual.com

800.637.2676 | cunamutual.com
P.O. Box 391 | 5910 Mineral Point Road
Madison, WI 53701-0391

CUNA MUTUAL GROUP