It appears there were just over 200,000 credit cards among the 143 million records potentially compromised. Equifax has indicated that debit cards were not exposed – therefore criminals are unlikely to immediately have the capability to withdraw funds from a checking account.

Affected consumers are at risk from criminals using stolen information to fraudulently open accounts. This means that the most immediate (and long-term) threat with this breach is identity theft, and the best thing credit unions can do is provide their members with identity protection tips.

The first step members should take to find out more is to visit Equifax's website. Equifax has a tool that can help consumers determine whether their data has been exposed. Then, consumers should take steps to protect their identity. These include:

- Don't respond to emails, texts or telephone calls asking for personal or financial information.
- Frequently review account activity and immediately report unauthorized transactions.
- Consider the 1 year of free ID theft protection being offered by Equifax to all Americans (note: There was initially an arbitration clause inserted in the language for the ID-theft monitoring service that Equifax was offering to all consumers. That language has been removed, and the company claims it does not apply in this case.)
- Place an initial fraud alert with a credit bureau, which is free and will apply to all the credit bureaus.
- Consider the benefits and drawbacks of credit freezes, which are more secure and longer-term than fraud alerts, but more restrictive.
- Always use multi-factor authentication when available.
- Update PINs and passwords, including email passwords, and follow best practices (i.e.: using long and complex phrases, and never re-using passwords).
- Enroll and opt-in for transaction monitoring.
- Use card on/off switches (if available).
- Enroll in Verified by VISA / MasterCard Secure Code.