DATA BREACH

AND

IDENTITY THEFT

INFORMATION FOR RESIDENTS

Lincoln County Sheriff's Office (207) 882 - 7332

A Word From Sheriff Brackett...

Each week, too many of our residents become victims of financial fraud – whether through a scam, a data breach or identity theft.

Scams, (also called "Crimes of Persuasion" because you have been persuaded to part with money or information) can happen on your phone, on your computer or even at your door.

Identity theft can involve the use of your social security number, date of birth, debit or credit card, bank account, license – even your medical information.

And a data breach can happen to any of us at any time without our knowledge.

We are providing this information for residents to help you protect your information and to minimize financial loss.

Sheriff Todd Brackett
Lincoln County Maine

Data Breaches

What information was exposed?

If any of these types of information was exposed, proceed to the next steps:

Debit or credit card
Bank account number
Social security Number
Date of birth
Driver's license number
State identification card number
Account passwords, pins or other access codes

1. If your bank account, debit or credit card information was exposed, contact the issuing bank immediately and report the breach. (You may have been contacted by the bank already.) Make sure that the card or account that was compromised is cancelled and that the bank issues a new one to you.

2. Ask the bank/credit card company to place an alert on your accounts so that you can approve any transactions *before* they happen.

3. If your bank account, debit card or credit card is automatically charged by a business as a way of making regular payments, make sure that you inform these companies that the account (or card) number has been changed so that your good credit isn't affected by the change in your card information.

4. If you shop online and have your debit card information stored with PayPal or with an internet seller, contact the business to provide them with updated information concerning your new card number. Because of protections afforded under federal laws, we strongly encourage you to use a credit card and NOT a debit card for any online transactions.

5. Be sure to destroy your old debit card and dispose of it so that it is inaccessible

6. Call the credit bureaus and place a 90-day fraud alert on your credit reports:

Equifax – 1-800-525-6285

Experian – 1-888-397-3742

Transunion – 1-800-680-7289

You will be asked to give them your social security number. The fraud alert process is an automated phone process, so you can call to place your fraud alert any time, 24 hours a day, seven days a week. For security reasons, please do not use the internet to place your fraud alert.

Order copies of your credit reports to review from The Federal Trade Commission's officially-recognized provider for your free credit reports:

Annual Credit Report.com

1-877-322-8228

We strongly suggest that you DO NOT order your credit reports online because of the concern about revealing your social security number over the internet.

7. Monitor your bank account and credit card statements for the period just before the breach and for the following months. Be sure to look for any small charges that may represent a "test" charge that a thief is using to test your card information. Report any unauthorized charges on your statement immediately.

8. If your Maine driver's license was compromised, the Bureau of Motor Vehicles asks that you contact their Office of Investigations and discuss the breach of your information with a member of the Office. They can be reached by calling:

State of Maine
Bureau of Motor Vehicles
Office of Investigations
207-624-9000 ext. 52144

9. If your social security number or date of birth was exposed, contact the Social Security Administration immediately at either their toll free main number (1-800-772-1213) or (TTY 1-800-325-0778) or by calling them at your local office. Explain that your Social Security Number was affected and that you are concerned about identity theft. The Social Security Administration does not automatically issue a new number to individuals if their information has been breached. However, if you receive Social Security benefits, you may be able to place a "block" on your information to make sure that a thief does not redirect your benefit to another address.

10. Place a security freeze on your credit reports.

Fraud alerts only last for 90 days and must be renewed by you at the end of that time. Security freezes offer more protection for you than the fraud alert. With a security freeze, you are issued a PIN (Personal Identification Number) and your credit information cannot be released to new creditors until you have been contacted and have authorized the release by giving your PIN.

In October, 2015, Maine became one of only a handful of states that allows residents to place a security freeze at all credit bureaus for free. In addition, the same revised law now allows parents of minor children to place a security freeze on a child's credit reports as well for free. This security freeze does not need to be renewed in 90 days and will prevent the unauthorized use of your or your child's information to open new credit accounts.

In September, 2017, Equifax announced a massive data breach that affected 145.5 million records.

Because of this breach, we advise Maine residents to contact the three credit bureaus (Equifax, Experian and TransUnion) to place a security freeze on their credit reports. In Maine, there is no charge to place the security freeze which is protected by state law, unlike "security locks" being offered.

For more information about placing a security freeze on your or your minor child's credit reports, here are the phone numbers to call:

Transunion – 1-888-909-8872

Experian – 1-888-397-3742

Equifax – 1-800-685-1111 Option 3

11. What about credit monitoring?
The "free" credit monitoring or "identity repair" services offered to victims by some companies that have sustained a breach do not protect you from certain types of identity theft, such as fraudulent use of your existing card number to make purchases and income tax identity theft which is now the fastest growing type of identity theft.

If you have been offered a free year of credit monitoring services, please stay vigilant – DO NOT ASSUME that the service will catch and stop all types of identity theft.

Ask the monitoring service how many credit bureaus are being monitored. Some credit monitoring includes only one credit bureau, rather than including all three. This may mean that information from the other two credit bureaus is not seen immediately by the credit monitoring company. It may take 30 days or longer the credit monitoring service learns about an attempt to use your information. In the meantime, identity thieves might be able to use your stolen information to obtain credit and establish accounts in your name.

For these reasons, we encourage you to place security freezes on your credit reports rather than rely on credit monitoring.

IDENTITY THEFT

1. If your credit card, debit or ATM card was involved, call the credit card company or your financial institution and report the unauthorized use of your card. Then call any companies where the thief made purchases or opened accounts using your information. Tell the fraud department that this was an unauthorized use of your card and that you are disputing the charges. Follow up by sending a dispute letter to creditors. Each creditor and your credit card company (if it was involved in the identity theft transaction/s) need to receive a dispute letter from you. Include a copy of your police report with the letter.

2. If you have reason to believe that your information was used to file a false return with the IRS, contact the IRS and report your concerns to them. Notify the IRS if they have not contacted you first. If they have contacted you, reply immediately to them at the phone number they provide. Please note: the IRS will initiate contact with you in writing – they will NOT contact you via email or phone.

You may be a victim of IRS fraud due to identity theft if the IRS informs you that more than one return has been filed under your social security number for a particular year, or if you owe taxes for a year in which you didn't file a return or if an employer you do not know claims that you were employed by him or her.

The IRS will send you an identity theft affidavit form to complete (Form 14039.) Complete this form and return it to the IRS with a copy of your police report.

3. Call local law enforcement and make a report. Tell the police that you will need a copy of the report. Make copies of the report and include one with each dispute letter you send to a creditor.

4. Contact the three credit reporting bureaus and place a fraud alert on your credit report with each bureau. Here are the phone numbers to contact them:

Equifax	1-800-525-6285
Experian	1-888-397-3742
Transunion	1-800-680-7289

Order copies of your credit reports to review from The Federal Trade Commission's officially-recognized provider for your free credit reports:

Annual Credit Report.com	1-877-322-8228

We strongly suggest that you DO NOT order your credit reports online because of the concern about revealing your social security number over the internet.

5. Monitor your account statements to make sure that there are no further fraudulent charges.

6. After 90 days the fraud alert you placed on your credit reports will expire. At that point, you may either extend the fraud alert for seven years or place a security freeze on your credit reports. In Maine, a security freeze is free to adults and children.

7. If your social security number was used or if benefits were fraudulently obtained using your or your child's information:

Contact the Social Security Administration immediately at either their toll free main number (1-800-772-1213) or (TTY 1-800-325-0778) or by calling them at your local office. Explain that your or your child's social security number was used to fraudulently obtain benefits. If you are concerned that someone has used your minor child's information to apply for and receive social security benefits, you may be able to place a "block" on your or your child's information.

Victims of identity theft are encouraged to contact Social Security by phone to discuss their unique situation before placing a block on their information. As an additional precaution, you may want to check your child's earnings information with the Social Security Administration. You may want to request this information every year so that you can discover if someone is using your child's social security number to obtain work.

If you would like to obtain a report, call 1-800-772-1213 or visit http://www.ssa.gov/online/ssa-7004.html

8. If the identity of a deceased family member was used:

To dispute this type of identity theft, you will need to have several copies of the death certificate and know the deceased person's social security number.

First, you should take steps to make sure that the Social Security Administration and the credit bureaus are notified about the death of your loved one. In order to do this, you should be either the surviving spouse or otherwise authorized to act on behalf of the deceased person. You can contact the Social Security Administration at one of their offices here in Maine.

Credit bureaus also need to be notified and you will need to request that the deceased person's credit file be marked ""Deceased. Do Not Issue Credit." The three credit bureaus will need a letter from you along with a copy of the death certificate.

9. Make sure that you receive letters or statements that show that the bank or creditors have credited fraudulent amounts to your account and that you are no longer liable for these.

10. Keep copies of all documents in a safe place for seven years.