Taking Steps to Help Protect Your Identity

In today's internet world, it is important to proactively take steps to protect the security of your personal information. At LeTort Trust, the security of your personal and financial information is our top priority. In addition to the rigorous measures we take, outlined in the attached LeTort IT Risk Management Program, there are steps you can take to help protect against Identity Theft and Fraud. Working together to protect identity theft is the best way to help keep your information safe and secure.

1. Lock up your social security card, birth certificate, passport, and other personal IDs that contain sensitive information. Do not carry these items with you (except when absolutely necessary, such as to travel to a foreign country).

2. Don't give account numbers, passwords, personal information via phone unless you have initiated the call. Do not give out your social security number (SSN) unless absolutely necessary. Ask for a different identifying number if the SSN is being used (such as for a state driver's license).

3. Destroy all documents containing personally identifying information when you dispose of them. In particular, make sure to destroy bank and credit card statements, expired credit cards, old tax documents, health insurance forms, medical records, and utility bills. If you use a shredder, use one that cross shreds for the best destruction.

4. Shred all credit card and mortgage offers. ID thieves can use them to apply for credit in your name. Better yet, call (1-888-567-8688) to opt out of receiving offers of credit based on your credit report.

5. Limit the number of credit cards you have and when cancelling credit cards not in use, follow the attached rules to avoid negative impacts on your credit score. Closing Credit Cards

6. Check credit card and bank statements each month as soon as they arrive or are available online. This is the best way to detect any unauthorized use, plus most credit card companies and financial institutions only allow you to challenge mistakes for a set period of time, typically
60 days. Also, ask credit card companies not to send you "convenience" checks that could easily be stolen.

7. Limit use of debit cards attached to your bank accounts. Try not to use them at restaurants (or anywhere else that they leave your sight) or for online transactions. Federal law, bank policies, and debit card issuers generally protect against most debit card losses, but the extent of the protection varies.

8. Pick up new checks at the bank instead of having them sent to your mailbox.

9. Keep an eye on your mail. Deposit outgoing mail in post office collection boxes, don't put it in your home mailbox if it is unsecured, and promptly remove delivered mail. Stop mail delivery when you go on vacation.

LETORT
TRUST

Taking Steps to Help Protect Your Identity

10. Check your credit report regularly to look for unauthorized credit applications. The Fair and Accurate Credit Transactions Act (FACTA), gives every person a free annual credit report. To get yours, visit Annual Credit Report or call toll-free 1-877-322-8228.

11. Do not respond to unsolicited email asking for personal information. Thieves often will send out emails that appear to be from legitimate entities, such as banks, asking you to provide personal information, account information, and passwords. Some even direct you to provide the info on "secure" fake Web sites that look authentic, using corporate logos, etc. Your bank or credit card issuer typically will not send out emails to ask for this type of information. If you really think it is from your bank, call them directly, but do not use a number provided on a suspicious email.

12. Protect your computer. Use, and update regularly, virus and firewall protections to prevent outside access to your computer. Also, use "strong" passwords to protect your financial and other personal information that mix letters and numbers. Change passwords regularly for added protection and keep any written record of your passwords in a secure place, not on your computer.

13. Destroy all personal and financial information on your computers before discarding or giving them away. Simply deleting the files is not enough, you must have the information deleted from storage or destroy the hard drive.

14. Immediately report any losses of personal identification and credit cards.

15. Consider purchasing special ID theft protection. ID theft protection plans typically monitor your credit report and report any suspicious activity. In the event of a theft, the best plans will help you file reports, dispute unauthorized activity, and restore your identity.

16. Consider setting up a credit freeze by contacting each the three major bureaus: Equifax, Experian or TransUnion. This step is not for everyone, and can delay you getting credit approval in the event you want to have a company access your credit report, but for some it is a good way to protect access to your credit report. The link below explains the process at Experian. You would need to do the same procedure for each of the other two credit bureaus. Experian Link to Credit Freeze

LETORT
TRUST

LeTort Trust Information Security Risk Program

LeTort maintains an Information Security Risk Program to create effective administrative, technical and physical safeguards in order to protect LeTort client non-public personal information. The IT Security Officer is responsible for this program.

The Information Security Risk Program will ensure the security and confidentiality of client information; protect against any anticipated threats or hazards to the security or integrity of client information; and protect against unauthorized access to or use of client information that could result in substantial harm or inconvenience to any LeTort client.

Directors or others shall, at least annually, review the Information Security Risk Program to evaluate its effectiveness to protect LeTort client information. This compliance may be based on the evaluation on the reports of internal personnel and/or external auditors.

The Trust and Administrative Committee is responsible for the Information Security Risk Program. The Committee may delegate day-to-day authorities to a Level 2 Authority or Network Administrator.

The Information Security Risk Program includes the following:

- **Annual review of Technology Policyy**
- **Annual review of Disaster Recovery Plan (Business Continuity) and testing results with specific reference to information security**
- **Annual review of LeTort Technology Plan**
- **Annual review of Vendor/Contract List**
- **Annual review of services performed by IT consultants and review of monthly reporting by those IT providers on the LeTort information security.**
- **Annual review of the IT Matrix Risk Assessment**
- **All employees will be provided annual training for Information Security Risk program and Security Awareness. Training topics will include, but not limited to, Data & Physical Security, Information Security, Data Communication and Transmission of client information**

Along with the IT Security Program, LeTort employs technical consultants to oversee, test and develop the measures to prevent unauthorized access to LeTort's network and data. Policies and procedures are in place for all use of data and communications network.

The LeTort network is protected by a central antivirus program, a state of the art CISCO firewall and numerous other data protection measures. Audits of the IT program and infrastructure are completed annually and as a non-depository financial institution, the State Banking Department completes its own audit of the LeTort Information Technology.

LETORT
TRUST