IDENTITY THEFT / COMPROMISED ACCOUNT RESOURCES

It's important to understand what is happening. Different situations require different procedures. Click the links below to jump to the appropriate section. Use the boxes to the left of each step to mark them as complete as you do them.

MY COMPUTER HAS BEEN "HACKED"

If your computer has been "hacked" or has a virus and you're not sure what to do, there are some simple steps you can follow that will start you on the right path and help ensure you're protected.

- ☐ Remain calm and collect your thoughts. Don't panic.
- ☐ Disconnect your computer from the Internet and shut it down to prevent further damage or use.
- ☐ Document everything and start a paper trail for "just in case" purposes.
- ☐ Change your passwords to online banking, email, and other services as soon as you have access to a different computer or phone.
- ☐ If you suspect your online banking or financial information has been compromised, contact FNB Bank and we'll help you with this.
- ☐ Contact an IT Support company yourself to get your computer professionally cleaned up. Don't answer unsolicited tech support calls. Scammers who may have your information may try to phish you over the phone or through text messages.
- ☐ Make sure you have data backups and that they work. Do not restore until after your computer is confirmed to be safe and cleaned up by a professional.
- ☐ If you have ransomware asking you to pay money to unlock your computer, do not pay it. This could be illegal under new guidance set forth by the Federal government.
- ☐ Make sure you have quality computer security software installed. Ask your IT Support company for recommendations, they can help you.
- ☐ Here are links from the US-CERT and Federal Trade Commission with additional help:
  US-CERT: Recovering from a Trojan Horse or Virus
  FTC: Get Rid of Malware

FNB
MEMBER FDIC

IDENTITY THEFT / COMPROMISED ACCOUNT RESOURCES

I HAVE FRAUDULENT CHARGES ON MY FNB DEBIT CARD

If you have fraudulent charges on one of your accounts, FNB can help you with this and there are some additional steps you'll need to take to make things easier:

- ☐ Remain calm and collect your thoughts. Don't panic.
- ☐ Document everything and start a paper trail.
- ☐ Change your passwords to websites and other places your debit card information was used (Amazon, utility companies, etc.)
- ☐ Contact FNB Bank over the phone or in person and explain the situation and the fraudulent charges to our staff. It's best if you have the known charges before you contact us but we can help you go through them as well.
- ☐ It's likely that we'll issue you a new debit card. Your old card will not be active any longer so websites and services that use the old card's numbers will need to be changed to your new card's information.
  Note: Most of our branches can print you a new debit card on the spot.
- ☐ Make sure you have FNB's online banking service and use it to keep a close eye on your accounts for the next 30-90 days to make sure it was only your previous card that was compromised and not the account itself.

I BELIEVE SOMEONE HAS MY ACCOUNT NUMBER(S)

If you believe your entire bank account has been compromised, this is slightly less common than just the debit card compromise and requires a bit more but FNB can help you, no problem:

- ☐ Remain calm and collect your thoughts. Don't panic.
- ☐ Document everything and start a paper trail.
- ☐ Change your passwords to websites and other places your debit card and banking information was used (Amazon, utility companies, etc.)
- ☐ Contact FNB Bank over the phone or in person and explain the situation to our staff.
- ☐ It's likely that we'll close your account on the spot and issue you all new account numbers including a new debit card. Your old card will not be active any longer so websites and services that use the old card's numbers or your old account information will need to be changed to your new card's information. This may include direct deposit with entities like your employer or Social Security.
  Note: Most of our branches can print you a new debit card on the spot.
- ☐ Make sure you have FNB's online banking service and use it to keep a close eye on your accounts for the next 30-90 days to make sure it was only your previous account information that was compromised.

FNB
MEMBER FDIC

IDENTITY THEFT / COMPROMISED ACCOUNT RESOURCES

MY IDENTITY HAS BEEN STOLEN

If you believe your identity has been stolen and is someone is opening accounts, getting loans, etc. under your name, this is a serious situation. The Federal Trade Commission offers free identity theft help with customized recovery plans at IdentityTheft.gov and FNB Bank can provide paper booklets in our branches to help as well. The steps below will get you started on your identity theft recovery:

- ☐ Remain calm and collect your thoughts. Don't panic.
- ☐ Document everything and start a paper trail. This includes who you contacted, when, and what was discussed.
- ☐ Contact FNB and explain the situation. We can give you new accounts and debit cards and place watches on your accounts.
- ☐ An FNB Bank employee can get you an identity theft recovery kit from the Federal Trade Commission if you can't or aren't comfortable using a computer.
- ☐ Call other companies where fraud occurred and explain that your identity was stolen.
- ☐ Contact one of the three credit bureaus and place a free fraud alert on your information. Contacting one of them should force them to share your request with the others but verify this.
  Experian.com (888-EXPERIAN; 888-397-3742)
  TransUnion.com (888-909-8872)
  Equifax.com (800-682-1111)
- ☐ Get your free credit report to review and make note of any transactions you don't recognize.
  Annualcreditreport.com (877-322-8228)
- ☐ Go to IdentityTheft.gov and start your free personalized recovery plan. Include as many details as possible. This will make your recovery plan more accurate and help law enforcement if they need to be involved.
- ☐ Contact the Social Security Administration to make them aware that your identity was stolen.
- ☐ Change your passwords to your email, online banking, and other websites you log into.
- ☐ Many of these steps are taken directly from the FTC's identity theft guides. Feel free to check the guides out. They can be found below for different types of identity theft to include Medical, Child, and Military identity theft:
  FTC: Identity Theft - A Recovery Plan
  FTC: Child Identity Theft
  FTC: Medical Identity Theft
  FTC: Military Personnel Identity Theft

FNB
MEMBER FDIC