Conducting Your Transactions Online

Federal financial regulators are reporting that Internet threats have changed significantly over the past several years. Sophisticated hacking techniques and growing organized cyber-criminal groups are increasingly targeting financial institutions, compromising security controls, and engaging in online account takeovers and fraudulent electronic funds transfers.

In order to help ensure the security of your online transactions, we want you to know that:

- We will never email, call or otherwise ask you for your user name, password or other electronic banking credentials
- You can help protect yourself by implementing alternative risk control processes like:
  - Making sure you choose an adequate user name and password that, at a minimum, mixes in small case letters, upper case letters and numbers
  - Periodically changing your password (e.g., at least every 90 days)
  - Safeguarding your user name and password information
  - Making sure you have a firewall in place when conducting your financial transactions
  - Logging off the system when you're done conducting business (don't just close the page or "X" out of the system)
  - Monitoring your account activity on a regular basis

In addition, we may require owners of commercial accounts to perform their own risk assessments and controls evaluations. For example:

- Make a list of the risks related to online transactions that your business faces including
  - Passwords being written down and left out in the open
  - The use of old or inadequate passwords
  - The possibility of internal fraud or theft
  - Delays in terminating the rights of former employees
  - The lack of dual control or other checks and balances over individual access to online transaction capabilities
- An evaluation of controls your business uses may include
  - Using password protected software to house passwords in
  - Conducting employee background checks
  - Initiating a policy and process to terminate access for former employees
  - Segregating duties among two or more people so no one person has too much access or control
  - Conducting internal or third party audits of controls
  - Using firewalls to protect from outside intrusion or hackers

Federal regulations provide consumers with some protections for electronic fund transfers. These regulations generally apply to accounts with Internet access. For example, these federal laws establish limits on a consumer's liability for unauthorized electronic fund transfers. They also provide specific steps you need to take to help resolve an error with your account. Note, however, that in order to take advantage of these protections, you must act in a timely manner. Make sure you notify us immediately if you believe your access information has been stolen or compromised. Also, review your account activity and periodic statement and promptly report any errors or unauthorized transactions. See the Electronic Fund Transfer disclosures that were provided at account opening for more information on these types of protections. These disclosures are also available online (or ask us and we will gladly provide you with a copy).

If you become aware of suspicious account activity, you should immediately contact the authorities and contact us at the number listed below.

CenterPointe
COMMUNITY BANK

What is Identity Theft?

Identity theft is a serious crime. It can disrupt your finances, credit history, and reputation, and take time, money, and patience to resolve. Identity theft happens when someone steals your personal information and uses it without your permission.

Identity thieves might:

- go through trash cans and dumpsters, stealing bills and documents that have sensitive information.
- work for businesses, medical offices, or government agencies, and steal personal information on the job.
- misuse the name of a legitimate business, and call or send emails that trick you into revealing personal information.
- pretend to offer a job, a loan, or an apartment, and ask you to send personal information to "qualify."
- steal your wallet, purse, backpack, or mail, and remove your credit cards, driver's license, passport, health insurance card, and other items that show personal information.

How to Protect Your Information

- Read your credit reports. You have a right to a free credit report every 12 months from each of the three nationwide credit reporting companies. Order all three reports at once, or order one report every four months. To order, go to annualcreditreport.com or call 1-877-322-8228.
- Read your bank, credit card, and account statements, and the explanation of medical benefits from your health plan. If a statement has mistakes or doesn't come on time, contact the business.
- Shred all documents that show personal, financial, and medical information before you throw them away.
- Don't respond to email, text, and phone messages that ask for personal information. Legitimate companies don't ask for information this way. Delete the messages.
- Create passwords that mix letters, numbers, and special characters. Don't use the same password for more than one account.
- If you shop or bank online, use websites that protect your financial information with encryption. An encrypted site has "https" at the beginning of the web address; "s" is for secure.
- If you use a public wireless network, don't send information to any website that isn't fully encrypted.
- Use anti-virus and anti-spyware software, and a firewall on your computer.
- Set your computer's operating system, web browser, and security system to update automatically.

If Your Identity is Stolen...

1 Flag Your Credit Reports

Call one of the nationwide credit reporting companies, and ask for a fraud alert on your credit report. The company you call must contact the other two so they can put fraud alerts on your files. An initial fraud alert is good for 90 days.

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

2 Order Your Credit Reports

Each company's credit report about you is slightly different, so order a report from each company. When you order, you must answer some questions to prove your identity. Read your reports carefully to see if the information is correct. If you see mistakes or signs of fraud, contact the credit reporting company.

3 Create an Identity Theft Report

An Identity Theft Report can help you get fraudulent information removed from your credit report, stop a company from collecting debts caused by identity theft, and get information about accounts a thief opened in your name. To create an Identity Theft Report:

- file a complaint with the FTC at ftc.gov/complaint or 1-877-438-4338; TTY: 1-866-653-4261. Your completed complaint is called an FTC Affidavit.
- take your FTC Affidavit to your local police, or to the police where the theft occurred, and file a police report. Get a copy of the police report.

The two documents comprise an Identity Theft Report.

COMMON WAYS ID THEFT HAPPENS:

Skilled identity thieves use a variety of methods to steal your personal information, including:

1. **Dumpster Diving.** They rummage through trash looking for bills or other paper with your personal information on it.
2. **Skimming.** They steal credit/debit card numbers by using a special storage device when processing your card.
3. **Phishing.** They pretend to be financial institutions or companies and send spam or pop-up messages to get you to reveal your personal information.
4. **Changing Your Address.** They divert your billing statements to another location by completing a "change-of-address" form.
5. **"Old-Fashioned" Stealing.** They steal wallets and purses; mail, including bank and credit card statements; pre-approved credit offers; and new checks or tax information. They steal personnel records from their employers, or bribe employees who have access.

DETER·DETECT·DEFEND

AVOID THEFT

www.ftc.gov/idtheft

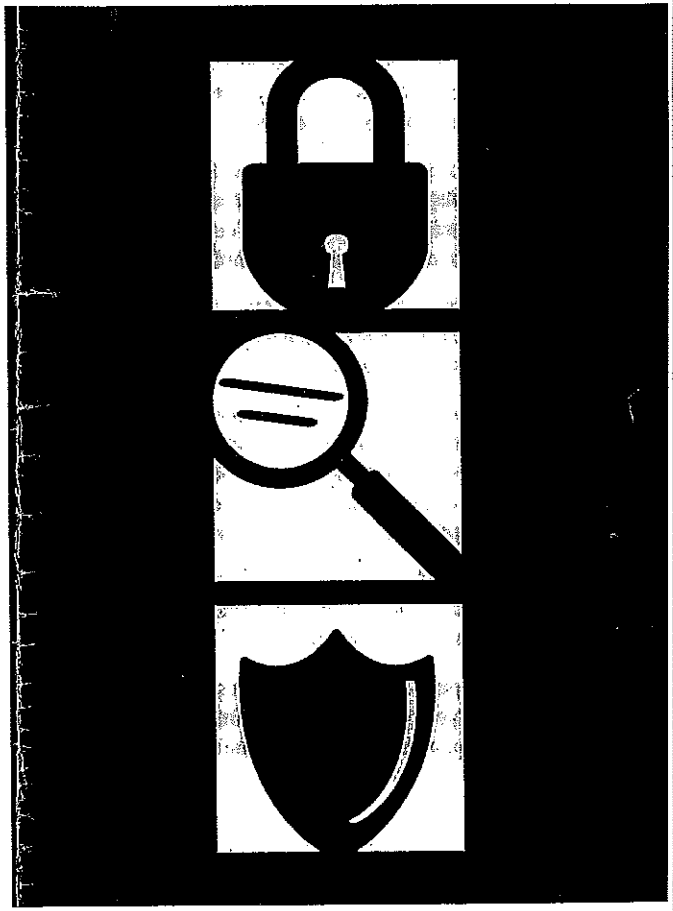
To learn more about ID theft and how to deter, detect, and defend against it, visit **ftc.gov/idtheft.** Or request copies of ID theft resources by writing to:

Consumer Response Center
Federal Trade Commission
600 Pennsylvania Ave., NW, H-130
Washington, DC 20580

DETER·DETECT·DEFEND

AVOID THEFT

www.ftc.gov/idtheft



FIGHTING BACK AGAINST IDENTITY THEFT

FEDERAL TRADE COMMISSION

DETER

Identity theft is a serious crime. It occurs when your personal information is stolen and used without your knowledge to commit fraud or other crimes. Identity theft can cost you time and money. It can destroy your credit and ruin your good name.

Deter identity thieves by safeguarding your information.

- **Shred** financial documents and paperwork with personal information before you discard them.
- **Protect** your Social Security number. Don't carry your Social Security card in your wallet or write your Social Security number on a check. Give it out only if absolutely necessary or ask to use another identifier.
- **Don't give out** personal information on the phone, through the mail, or over the Internet unless you know who you are dealing with.
- **Never click** on links sent in unsolicited emails; instead, type in a web address you know. Use firewalls, anti-spyware, and anti-virus software to protect your home computer; keep them up-to-date. Visit **OnGuardOnline.gov** for more information.
- **Don't use** an obvious password like your birth date, your mother's maiden name, or the last four digits of your Social Security number.
- **Keep** your personal information in a secure place at home, especially if you have roommates, employ outside help, or are having work done in your house.

DETECT

Detect suspicious activity by routinely monitoring your financial accounts and billing statements.

Be alert to signs that require immediate attention:

- Bills that do not arrive as expected
- Unexpected credit cards or account statements
- Denials of credit for no apparent reason
- Calls or letters about purchases you did not make

Inspect:

- **Your credit report.** Credit reports contain information about you, including what accounts you have and your bill paying history.
  - The law requires the major nationwide consumer reporting companies—Equifax, Experian, and TransUnion—to give you a free copy of your credit report each year if you ask for it.
  - Visit **www.AnnualCreditReport.com** or call 1-877-322-8228, a service created by these three companies, to order your free credit reports each year. You also can write: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.
- **Your financial statements.** Review financial accounts and billing statements regularly, looking for charges you did not make.

DEFEND

Defend against ID theft as soon as you suspect it.

- **Place a "Fraud Alert" on your credit reports, and review the reports carefully.** The alert tells creditors to follow certain procedures before they open new accounts in your name or make changes to your existing accounts. The three nationwide consumer reporting companies have toll-free numbers for placing an initial 90-day fraud alert; a call to one company is sufficient:
  - **Equifax:** 1-800-525-6285
  - **Experian:** 1-888-EXPERIAN (397-3742)
  - **TransUnion:** 1-800-680-7289

  Placing a fraud alert entitles you to free copies of your credit reports. Look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain.
- **Close accounts.** Close any accounts that have been tampered with or established fraudulently.
  - Call the security or fraud departments of each company where an account was opened or changed without your okay. Follow up in writing, with copies of supporting documents.
  - Use the ID Theft Affidavit at **ftc.gov/idtheft** to support your written statement.
  - Ask for verification that the disputed account has been closed and the fraudulent debts discharged.
  - Keep copies of documents and records of your conversations about the theft.
- **File a police report.** File a report with law enforcement officials to help you with creditors who may want proof of the crime.
- **Report the theft to the Federal Trade Commission.** Your report helps law enforcement officials across the country in their investigations.
  - Online: **ftc.gov/idtheft**
  - By phone: 1-877-ID-THEFT (438-4338) or TTY, 1-866-653-4261
  - By mail: Identity Theft Clearinghouse, Federal Trade Commission, Washington, DC 20580

DETER·DETECT·DEFEND

AVOID THEFT

www.ftc.gov/idtheft