Fraud Prevention and Security Procedures

Recognizing Fraud

Common Fraud Types

1. Unauthorized Credit/Debit Card Charges

Signs:

- Charges you don't recognize
- Duplicate charges for same purchase
- Charges from unfamiliar merchants
- Small "test" charges (fraudsters testing if card works)
- Charges from foreign countries you haven't visited

Immediate Actions:

1. Call 1-800-FRAUD-00 immediately (24/7)
2. Lock card in mobile app if available
3. Don't wait - early reporting prevents further charges
4. Note date, time, merchant name, and amount of fraudulent charges

2. Check Fraud

Signs:

- Missing checks from checkbook
- Checks clearing that you didn't write
- Altered check amounts
- Forged signatures

Report Immediately:

- Call 1-800-BANK-HELP
- File police report
- Submit affidavit of forgery (we'll provide form)

3. Account Takeover

Signs:

- Can't log into online banking (password changed)
- Unrecognized password reset emails
- Contact information changed without your knowledge
- Email/phone number updated
- New external accounts linked
- Unfamiliar devices accessing account

Immediate Actions:

1. Call 1-800-FRAUD-00 immediately
2. Don't use online banking - call only
3. Change passwords on email account
4. Review all recent account activity

4. Wire Transfer Fraud

Common Scenario:

- Email appears to be from known contact (vendor, title company, etc.)
- Requests wire transfer with "updated" banking information
- Urgent tone, pressure to act quickly

Red Flags:

- Unexpected wire transfer request
- Change in payment method
- Slight variation in email address (john@company.com vs john@cornpany.com)
- Request to keep transaction confidential
- Pressure or urgency

Verification Steps:

1. ALWAYS call known phone number (not number in email) to verify
2. Don't trust email alone for wire instructions
3. Verbally confirm all wire details
4. Use established contact information, not info from the request

5. Phishing and Social Engineering

Email Phishing Signs:

- Claims account compromised or "urgent action needed"
- Suspicious sender address (support@ourbank-secure.com vs legitimate @ourbank.com)
- Generic greeting ("Dear Customer" vs your name)
- Spelling/grammar errors
- Requests for personal information
- Links to fake websites
- Urgent deadlines ("within 24 hours or account closed")

Phone Phishing (Vishing) Signs:

- Caller claims to be from bank fraud department
- Asks for full account number, SSN, or password
- Requests one-time authentication codes
- Pressures immediate action
- Threatens account closure

Text Phishing (Smishing) Signs:

- "Click here to verify account"
- "Your card has been locked - call this number"
- Links to websites (hover to check actual URL)

What We'll NEVER Ask For:

- Full password or PIN
- Full Social Security Number (may ask for last 4 digits only)

- One-time authentication codes
- Remote access to your computer
- Gift card purchases to "secure" your account

Fraud Response Procedures

Debit Card Fraud

Step-by-Step Process:
1. Report Immediately: 1-800-FRAUD-00 (24/7)
    - Within 2 business days: $50 maximum liability
    - Within 60 days: Up to $500 liability
    - After 60 days: Potentially full loss
2. Card Deactivation: Happens immediately upon report
3. Provisional Credit:
    - Issued within 10 business days
    - For disputes over $50
    - While investigation ongoing
4. Fraud Affidavit:
    - Complete and return within 10 days
    - Available online, email, or mail
    - Describes fraudulent transactions
5. Investigation:
    - Completed within 45 days (90 days for new accounts)
    - Merchant contacted for transaction details
    - You may be asked for additional information
6. Resolution:
    - Fraudulent charges removed permanently
    - Or provisional credit reversed if charges deemed legitimate
    - Written notice of decision sent
7. New Card:
    - Standard delivery: 7-10 business days
    - Expedited: 2-3 business days ($25 fee, waived for fraud)
    - Temporary card available at branch immediately

Credit Card Fraud

Process Similar to Debit with Key Differences:
- **$0 Liability**: No liability for unauthorized charges when reported promptly
- **Faster Provisional Credit**: Often within 1-2 billing cycles

- **Keep Using Card**: New card number issued but may continue using if card not lost/stolen (for online fraud)

ACH/Check Fraud

Unauthorized ACH Debits:
1. Report within 60 days of statement date
2. File unauthorized ACH claim
3. Investigation: 10 business days
4. Credit issued if confirmed fraud
5. ACH block placed on merchant if desired

Forged/Altered Checks:
1. Report immediately upon discovery
2. File forgery affidavit
3. Police report recommended
4. Investigation: 30-45 days
5. Credit issued if signature/amount verification confirms fraud

Wire Transfer Fraud

Critical Timing:
- **Within 24 hours of sending**: Good chance of recovery
- **After 24 hours**: Very difficult, often impossible

Immediate Steps:
1. Call 1-800-FRAUD-00 immediately
2. Request wire recall (no guarantee of success)
3. Contact receiving bank (we'll provide details)
4. File police report
5. Report to FBI's IC3: www.ic3.gov

Prevention:
- Always verbally verify wire instructions
- Call known number, don't use contact info from email
- Establish callback procedures for wire requests

Identity Theft

If You're a Victim:
1. Call Us: 1-800-FRAUD-00
   - Place fraud alert on account
   - Review all recent transactions
   - Change online banking credentials
   - Issue new cards

2. File Reports:

- FTC: www.identitytheft.gov
- Police report (needed for fraud affidavits)
- Credit bureaus (fraud alerts and credit freezes)

3. Credit Bureaus:
   - **Equifax**: 1-800-525-6285
   - **Experian**: 1-888-397-3742
   - **TransUnion**: 1-800-680-7289
   - Place fraud alert (free, lasts 1 year)
   - Consider credit freeze

4. Monitor:
   - Check credit reports regularly (free at annualcreditreport.com)
   - Watch for new account openings
   - Review all bank statements closely

5. Recovery Plan:
   - Close fraudulent accounts
   - Dispute fraudulent charges
   - Consider identity theft protection service
   - Keep detailed records of all communications

Fraud Prevention Tips

Protect Your Cards

Physical Security:
- Never leave card unattended
- Shield PIN when entering at ATM/store
- Don't write PIN on card or keep in wallet
- Sign back of card immediately
- Report lost/stolen within 24 hours

Online Shopping Safety:
- Use credit card (not debit) for online purchases
- Shop only on secure websites (https:// and padlock icon)
- Avoid public WiFi for banking/shopping
- Use virtual card numbers if available
- Monitor accounts after online purchases
- Save confirmation emails

Card Skimming Prevention:
- Check ATM/gas pump for tampering:
- Loose card reader
- Unusual devices attached
- Different color/material than surrounding area
- Cover keypad when entering PIN

- Use ATMs in well-lit, high-traffic areas
- Prefer bank ATMs over standalone
- Check for hidden cameras above keypad

Protect Your Account Information

Password Security:

- Use unique password for banking (don't reuse)
- 12+ characters with mix of letters, numbers, symbols
- Change every 90 days
- Never share with anyone
- Don't save in browser on shared computers
- Use password manager

Two-Factor Authentication:

- Always enable 2FA
- Never share one-time codes
- Use authenticator app (more secure than SMS)
- Save backup codes in secure location

Personal Information:

- Don't share account number, SSN, or full card number unless you initiated contact
- Shred documents with account information
- Don't email sensitive information
- Be cautious on social media (avoid sharing too much personal info)

Recognize Scams

Common Scam Tactics:

1. Urgency: "Act now or account will close"
2. Fear: "Your account has been compromised"
3. Too Good to Be True: "You've won a prize"
4. Authority: "This is the IRS/FBI/Bank Security"
5. Secrecy: "Don't tell anyone about this"

Red Flags:

- Unsolicited contact requesting information
- Request for remote access to your computer
- Pressure to act immediately
- Unusual payment methods (gift cards, wire transfer, cryptocurrency)
- Requests to move money to "safe" account

If Contacted Suspiciously:

1. Don't provide any information
2. Hang up/delete email
3. Call us directly at official number: 1-800-BANK-HELP
4. Report scam attempt to us
5. Report to FTC: reportfraud.ftc.gov

Monitor Your Accounts

Daily Habits:

- Check account balance daily via mobile app
- Review transactions 2-3 times per week
- Set up account alerts:
- Low balance
- Large transactions (over $500)
- Foreign transactions
- Card not present transactions
- Password changes
- New external account linked

Monthly Review:

- Review full statement line by line
- Verify all withdrawals and deposits
- Check pending transactions
- Confirm payees and transfer recipients
- Look for small unauthorized charges (common fraud test)

Immediate Reporting:

- Report ANY suspicious activity within 24 hours
- Don't wait to investigate yourself
- Better to report and be wrong than delay

Account Security Features

Debit Card Controls (Mobile App)

- **Card Lock**: Instantly disable card
- **Transaction Limits**: Set daily spending limits
- **Category Controls**: Block gas, online, international, etc.
- **Location-Based**: Auto-lock when outside home area

Alerts and Notifications

- **Text Alerts**: Real-time transaction notifications
- **Email Alerts**: Daily summaries
- **Push Notifications**: Through mobile app
- **Customizable**: Set thresholds and types

Travel Notifications

Why Important: Prevents legitimate transactions from being blocked

How to Set:
1. Online banking: Profile > Travel Plans
2. Mobile app: Settings > Travel Notifications
3. Call: 1-800-BANK-HELP
4. Specify: dates and locations

What to Include:
- Countries/states visiting
- Departure and return dates
- International vs domestic

Fraud Monitoring

Automatic Protection:
- 24/7 transaction monitoring
- AI-powered fraud detection
- Suspicious activity flagged automatically
- Verification call/text if unusual activity detected

How to Respond to Fraud Alerts:
- Answer calls from 1-800-FRAUD-00
- Reply to text alerts (legitimate only from our official number)
- Never call number in suspicious email
- Confirm or deny transactions when asked

Dispute Resolution

Merchant Disputes (Non-Fraud)

Qualifying Disputes:
- Charged wrong amount
- Item not received
- Item significantly different than described
- Double charged
- Charged after cancellation
- Service not provided

Process:
1. Try Merchant First: Contact merchant for refund
2. File Dispute: If merchant doesn't resolve within 7 days
   - Online: Through online banking
   - Phone: 1-800-CARD-HELP
   - Branch: Visit any location
3. Provide Documentation:
   - Receipts

- Emails/correspondence with merchant
- Photos of product (if defective)
- Tracking information
- Cancellation confirmation

4. Provisional Credit: Issued within 10 business days (if over $50)
5. Investigation: 45-90 days
6. Resolution:
    - Dispute upheld: Credit becomes permanent
    - Dispute denied: Credit reversed, detailed explanation provided

Time Limits:

- Debit card: 60 days from statement date
- Credit card: 120 days from transaction date

Billing Errors

Examples:

- Incorrect amount posted
- Transaction not recognized
- Calculation error
- Failure to post payment

Report Within: 60 days of statement date

Resolution: 30 days for most issues

Compromised Information

If Debit/Credit Card Compromised

1. Immediate: Lock card in app
2. Report: Call 1-800-FRAUD-00
3. Review: Check recent transactions for fraud
4. New Card: Request replacement
5. Update: Change autopay information for recurring charges

If Online Banking Compromised

1. Change Password: Immediately if still able to access
2. Call: 1-800-TECH-HELP if locked out
3. Review: Check all recent transactions, external accounts, payees
4. Reset: All security questions
5. Enable: 2FA if not already active
6. Monitor: Watch account closely for next 30 days

If Check Information Compromised

1. Report: Call 1-800-BANK-HELP
2. Stop Payment: On any outstanding checks
3. Order New Checks: With different starting number
4. Consider: Closing account and opening new one if many checks stolen
5. Monitor: Watch for fraudulent checks clearing

Legal Protections

Regulation E (Debit Card/ACH)

Your Rights:

- Limit liability to $50 if reported within 2 business days
- Bank must investigate disputes
- Provisional credit during investigation
- Written resolution notice required

Regulation Z (Credit Card)

Your Rights:

- $0 liability for unauthorized charges
- Right to dispute billing errors
- Right to withhold payment on disputed amounts
- Can't be billed while dispute under investigation

FDIC Insurance

What's Covered:

- Deposits up to $250,000 per depositor
- Separate coverage for different account types:
- Individual accounts
- Joint accounts
- Retirement accounts
- Trust accounts

Not Covered:

- Losses due to fraud (but bank has fraud resolution processes)
- Stock/bond/mutual fund investments
- Safe deposit box contents

Additional Resources

Reporting Fraud Externally

Federal Trade Commission:
- Website: www.identitytheft.gov
- Phone: 1-877-ID-THEFT (1-877-438-4338)

FBI Internet Crime Complaint Center:
- Website: www.ic3.gov
- For cyber crimes, online fraud

Social Security Administration (if SSN compromised):
- Fraud Hotline: 1-800-269-0271

IRS (if tax-related fraud):
- Identity Theft Hotline: 1-800-908-4490

Educational Resources

- **Bank Website**: www.ourbank.com/security
- **Videos**: Fraud prevention tutorials
- **Workshops**: Free monthly webinars on security
- **Newsletter**: Monthly security tips (opt-in)

Elder Fraud Protection

Special Services for Seniors:
- Trusted contact person on file
- Dual authorization for large transactions (optional)
- Fraud alert calls on unusual activity
- Educational seminars at branches

Reporting Elder Financial Abuse:
- Bank: 1-800-FRAUD-00
- Adult Protective Services: (varies by state)
- National Elder Fraud Hotline: 1-833-FRAUD-11

Contact Information Summary

24/7 Fraud Hotline: 1-800-FRAUD-00
Card Services: 1-800-CARD-HELP
General Banking: 1-800-BANK-HELP
Technical Support: 1-800-TECH-HELP
Report Phishing: phishing@ourbank.com

Remember: We will NEVER ask for your full password, PIN, or one-time codes. When in doubt, hang up and call us directly at our official numbers above.