BANKING & FRAUD 101

John Fick, MLS, CFE, CFCI, CECFE

Lesson Outline

- Check Basics
- ACH Basics
- Wire Transaction Basics
- Online Banking Basics
- ATM/Debit Card Basics
- Regulations for Banks
- Resources





Learning Objectives

- Understand Check Fraud Basics: Understand the check processing process through the Federal Reserve, Identify common types of check fraud, and recognize key best practices to prevent fraudulent checks

- Explain ACH Fraud Fundamentals: Describe how Automated Clearing House (ACH) transactions work, recognize typical fraud schemes targeting ACH systems, and apply best practices for preventing and detecting unauthorized transactions

- Recognize Wire Transfer Fraud: Understand the wire transfer process, identify common wire fraud scams, and implement controls to mitigate the risk of fraudulent wire transfers

- Identify ATM Fraud Techniques: Explain the functionality of ATMs, recognize common fraud schemes, and apply measures to protect ATM transactions and infrastructure

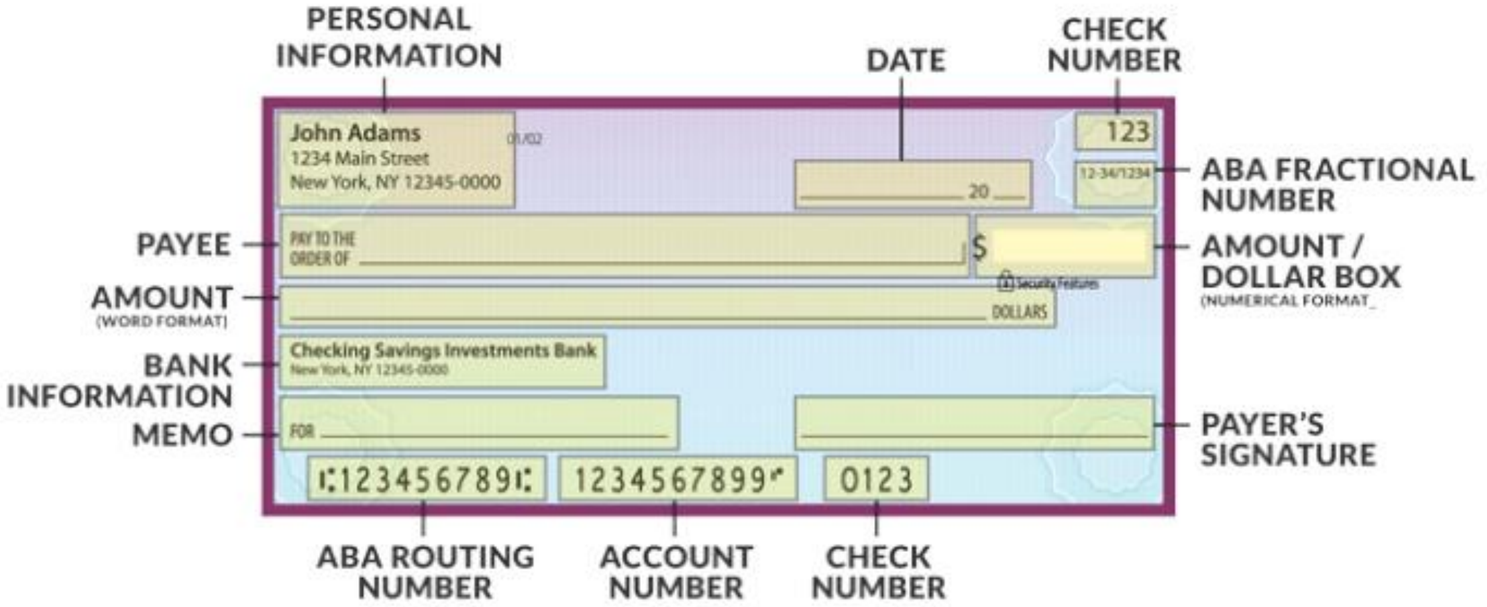
- Apply Key Banking Regulations: Understand essential banking regulations related to banks and fraud prevention and detection, including the Bank Secrecy Act (BSA), Regulation CC, Regulation E, and the Uniform Commercial Code (UCC), and ensure compliance in fraud investigation and prevention efforts

CHECK BASICS



Check Basics

What are the Elements of a Check?



The ABA fractional number, along with the MICR line, allows banks to quickly and accurately process checks and identify the bank responsible for paying them.

Numerator:
The top part of the fraction. It's a five-digit number with a hyphen separating the first two digits from the remaining three.

- The first two digits before the hyphen are the City/State Prefix.

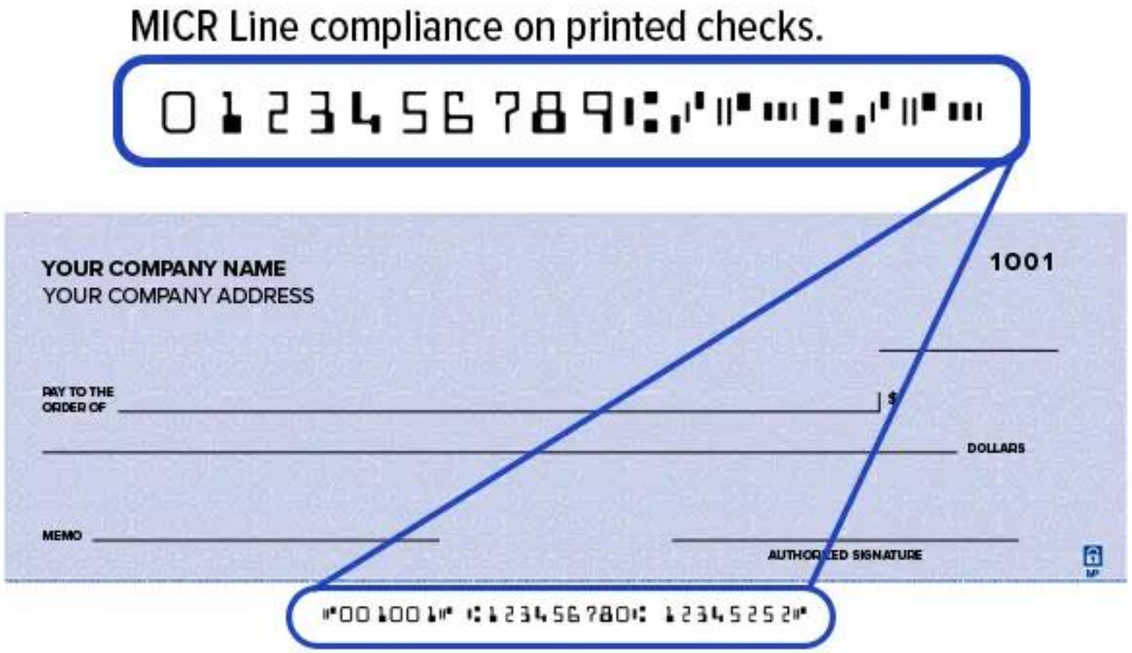
- The three digits after the hyphen are the ABA Institution Identifier.

Denominator:

The bottom part of the fraction. It's a three or four-digit number representing the Federal Reserve Routing Symbol.

Check Basics

What are the Elements of a Check?



The MICR line can vary in sequence of information:

Account Number – Routing Number – Check Number
Check Number – Routing Number – Account Number
Routing Number – Account Number – Check Number

DDA – Demand Deposit Account - Bank Account Number
ABA – Bank Routing Number – Unique code assigned by the American Bankers Association

Check Basics

What are the Elements of a Check?



Once negotiated, the back of the check contains valuable information

1. Endorsement (Payee, blank, restrictive, FBO, Mobile, Business, conditional)

2. Bank of First Deposit - (BOFD) typically includes name and routing number of the BOFD
   a. Sequence numbers, etc.

Check Basics - Fed Process

01

Check Deposit & Collection

- A check is deposited at the **Depository Bank**
- It’s scanned and converted to an **electronic image**

02

Submission to the Federal Reserve

- The check is sent to the **Federal Reserve Bank**
- The Fed acts as an **intermediary** between banks

03

Routing & Clearing

- The Fed identifies the **Paying Bank** using the check’s **routing number**
- The check is forwarded for **verification**

04

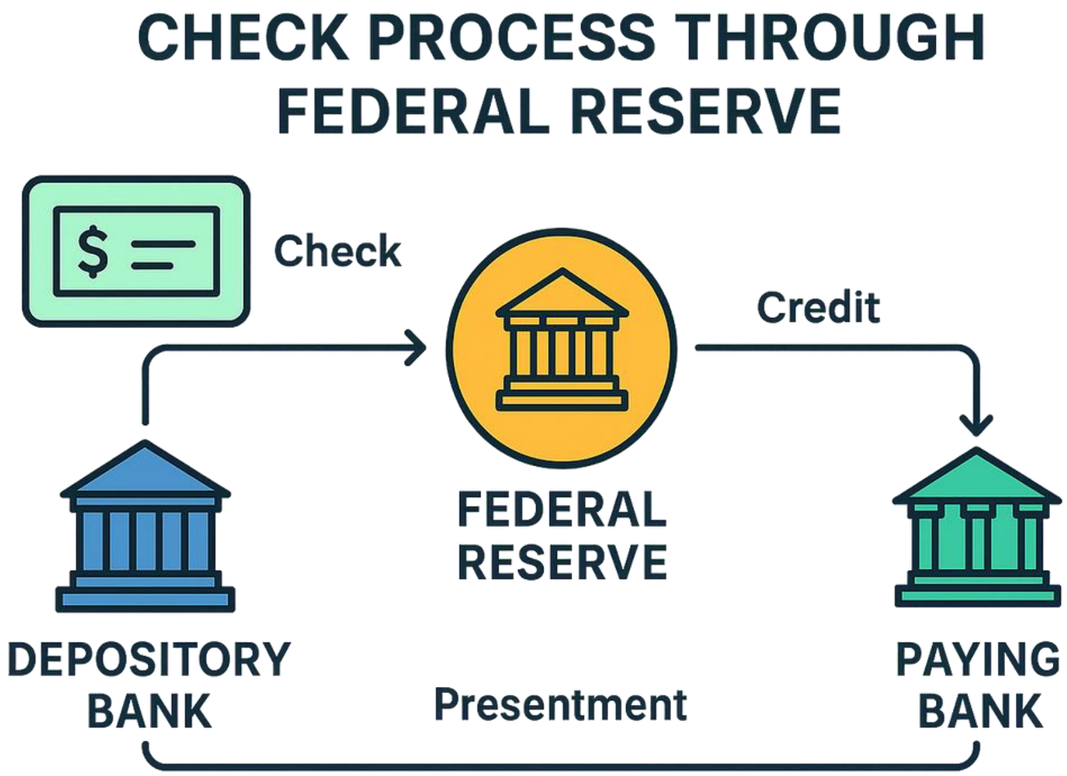
Settlement & Funds Transfer

- The Paying Bank **reviews & approves** the check
- Funds are **debited** from the check writer’s account
- The Fed processes the settlement via **Fedwire**

05

Final Posting & Confirmation

- Funds are **credited** to the Depository Bank
- The payee’s account is **credited**
- Process completes within **one business day**



Check Basics - Fed Process

Structure & Purpose

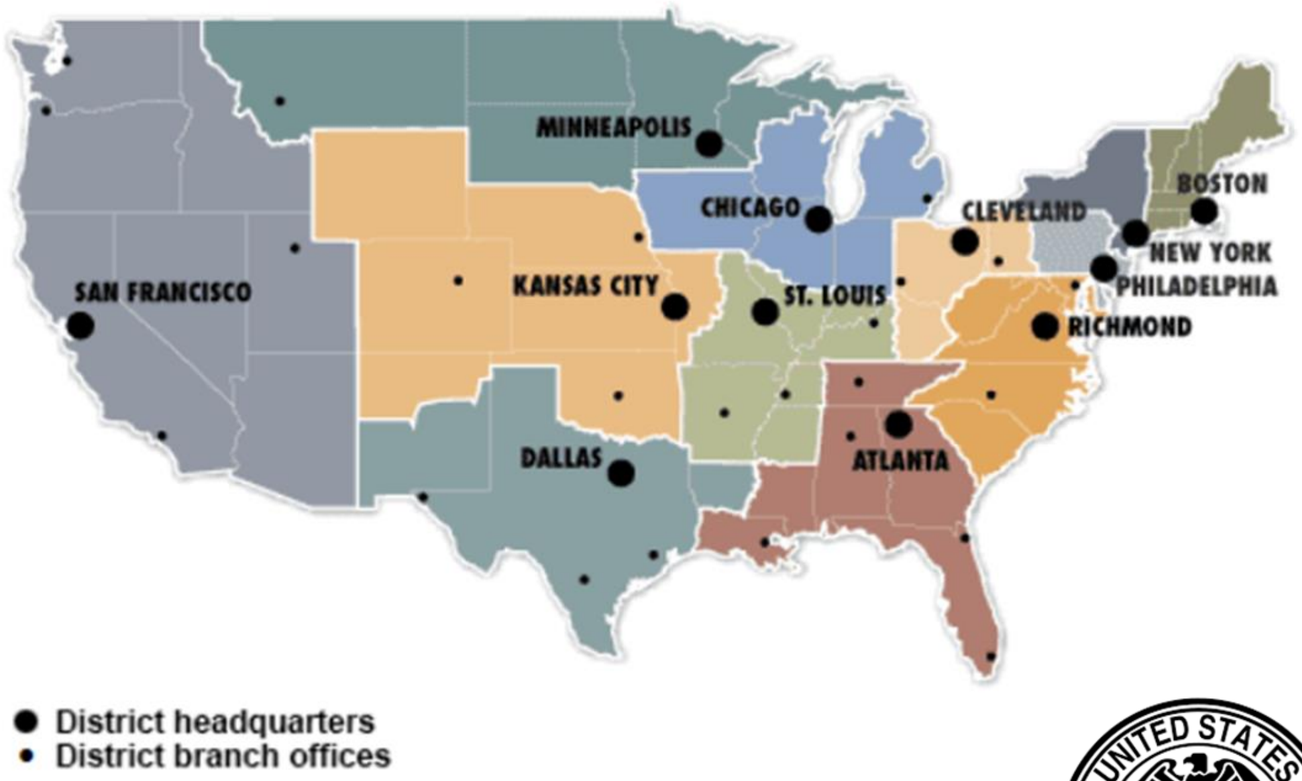
- Established in 1913 to stabilize the economy
- Composed of 12 regional Federal Reserve Banks
- Overseen by the Federal Reserve Board of Governors

Influence on the Economy

- Sets interest rates to guide borrowing & spending
- Maintains price stability through inflation control
- Supports employment growth through monetary policies

Key Responsibilities

- Monetary Policy: Adjusts interest rates to control inflation & economic growth
- Bank Regulation: Ensures banks operate safely & soundly
- Payment Processing: Facilitates check clearing & electronic transfers
- Financial Stability: Responds to crises & supports the economy



How Does Check Fraud Occur?



Car Break-ins



Office Creeps



Dumpster DIving



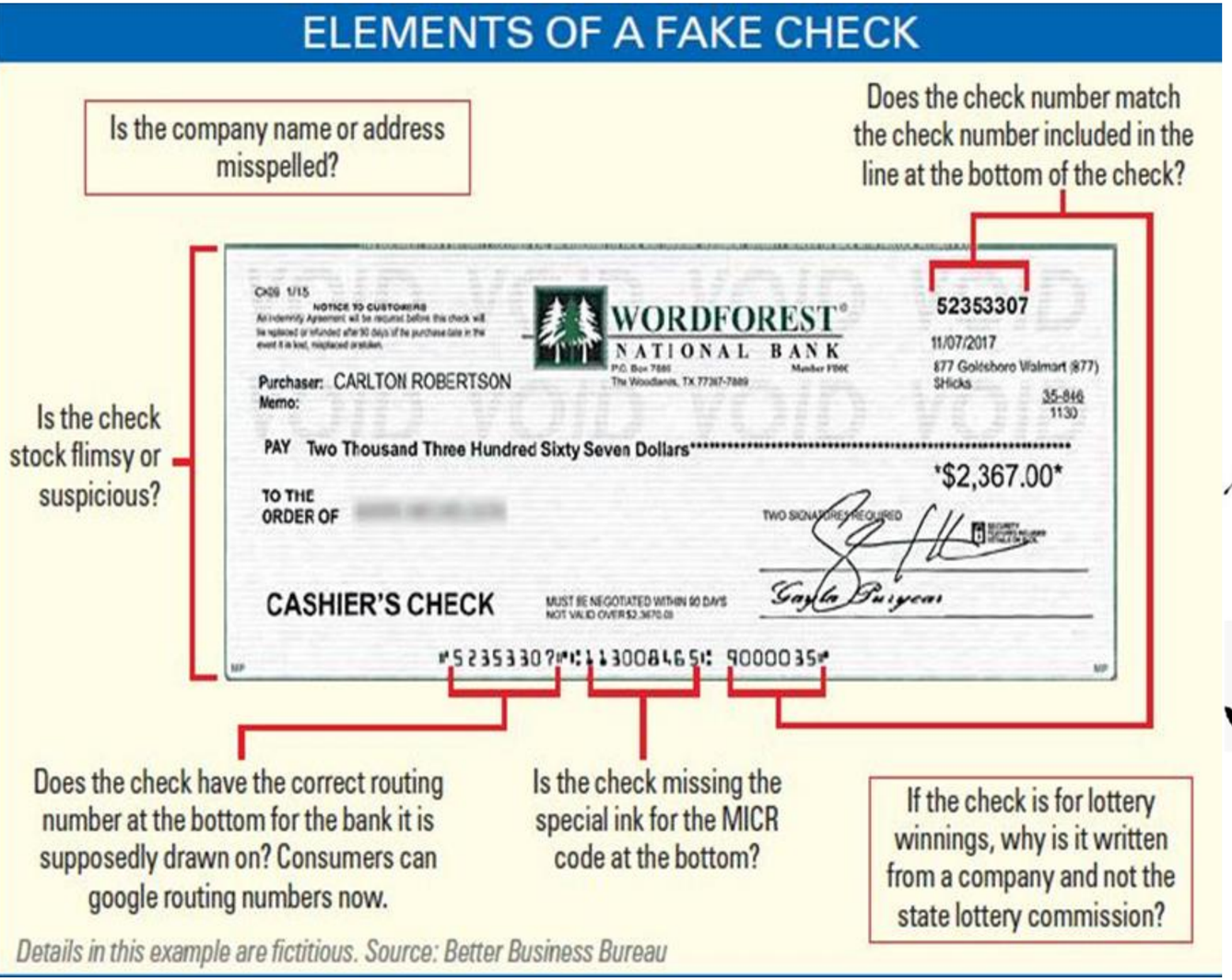
Mail Theft





Social Media

Check Fraud Red Flags





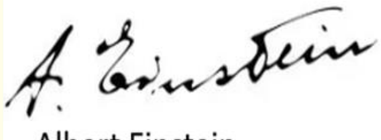
George Washington



Abraham Lincoln



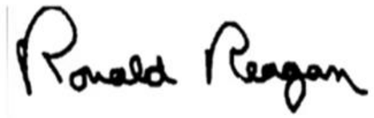
Robert Mugabe



Albert Einstein



Richard Nixon



Ronald Reagan



Salvador Dali



Martin Luther King, Jr.



Robert Redford

Check Basics - Kiting

DEFINITION

Check kiting is a form of fraud that exploits the time it takes for checks to clear between bank accounts.

HOW IT WORKS

- A person writes a check from Bank A with insufficient funds
- Deposits the check into Bank B
- Withdraws the funds from Bank B before the check from Bank A bounces

GOAL

To falsely inflate account balances and access funds that don't actually exist.

WHY IT'S ILLEGAL

- Creates the illusion of available money
- Results in financial loss to banks
- Considered bank fraud and a federal offense

COMMON RED FLAGS

- Frequent deposits and withdrawals between multiple accounts
- Large check amounts with rapid access to funds
- Accounts opened with minimal



Positive Pay Products



Positive Pay

Positive Pay solution protects business clients from unauthorized checks posting to the clients' accounts. The client rejects or approve the item before posting

Payee Positive Pay

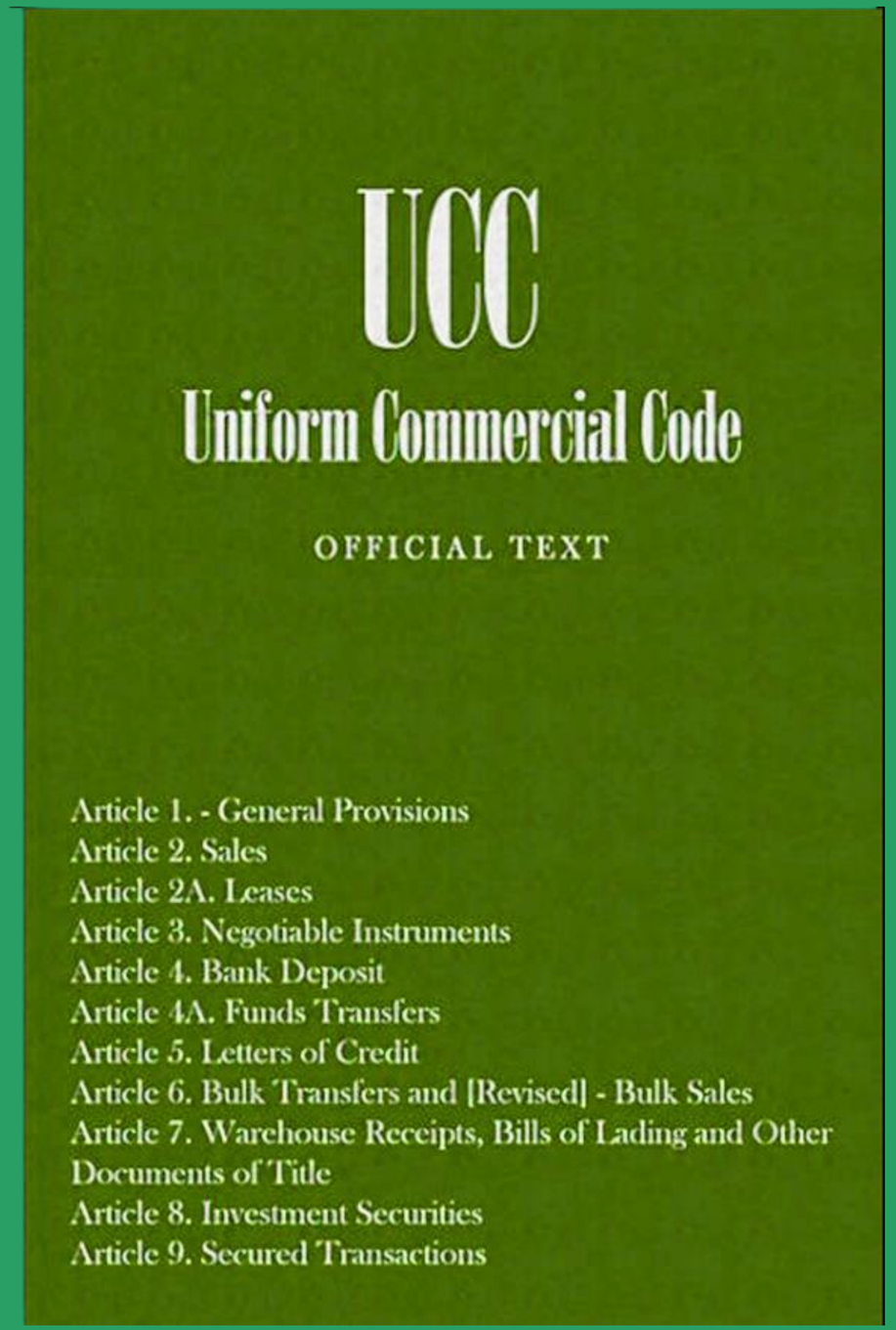
Like Positive Pay, Positive Pay with Payee match enabled, the clients upload a check issue file that includes the check number, amount, date, and payee name of the checks issued

Reverse Positive Pay

Reverse Positive Pay allows clients the ability to quickly review and compare items issued against checks paid and offers the option to export a file of paid checks for reconciliation

ACH FIlters & Blocks

ACH Positive Pay allows clients the ability to block all ACH debits or filter transactions allowing only those ACH debits they have authorized



Uniform Commercial Code

1

UCC Article 3 – Negotiable Instruments

- Governs the creation, transfer, and enforcement of checks
- Defines roles and responsibilities of parties involved (drawer, drawee, endorser, etc.)

2

UCC § 3-401 to § 3-407 – Signature and Fraud

- Covers unauthorized signatures, alterations, and forgeries
- States that forged or altered checks are not valid obligations of the account holder

3

UCC § 3-418 – Payment by Mistake

- Addresses the bank's right to recover funds paid out on forged or fraudulent checks

4

UCC § 4-401 – When Bank May Charge Customer's Account

- A bank cannot debit a customer's account for a check unless it is properly payable

Why It Matters:

- **Helps determine liability in check fraud cases**
- **Provides a legal framework for banks, businesses, and consumers to resolve disputes**

Check Basics - Check Fraud Types

	Return Time Frame Under the UCC:	HHL or BoW?
Forged Maker Signature – stolen and forged – often perpetrated by someone the victim knows	24 Hours	Hold Harmless Agreement
Alteration – checks stolen, washed, or manually altered, then negotiated. These are also often negotiated in the ATM or mobile deposit to avoid detection	1 Year	Breach of Warranty
Counterfeit – counterfeit checks drawn on legitimate accounts – often associated with scams such as online jobs and lottery/sweepstakes	24 Hours	Hold Harmless Agreement
Forged Endorsement – check stolen, endorsed, and negotiated by someone other than the payee - Often these checks are intercepted in the mail then negotiated via ATM or mobile deposits to avoid detection	3 Years	Breach of Warranty

Reporting Check Fraud



Customer must report the fraud to their bank & law enforcement



·Complete a Fraud Affidavit (Legal Document)

- Document what happened
- Provide the check number, check date, amount, payee & posting date
- Attest that they did not benefit financially from the fraudulent item
- Identify if they know the subject who negotiated the check
- Attest that, if necessary, they will voluntarily assist the bank and LE in the investigation and participate as a witness in any civil or criminal actions related to the incident

Check Fraud Investigation

Mitigating Check Fraud Bank Losses



- Review and determine and confirm the fraud type (counterfeit, forgery, alerted, forged endorsement)
- Type of check: Remotely Created, ARC, Cashiers Check, handwritten item, eCheck, etc.
- Can the check(s) in question be returned via the FED?
- Are we covered under the UCC Articles 3 & 4? Return time frames or Repeater rule?

Review Bank Agreements to determine if the customer:

- Uses Facsimile signatures
- Does the customer have Positive Pay?
- Is past the time frame to dispute the check (did the customer review their statements timely?)
- Secures their checks at their home/work/other location where they are kept

ACH BASICS



ACH Key Terms Defined

NACHA (National Automated Clearing House Association): NACHA is the governing body that manages the development, administration, and rules of the ACH network in the United States. It sets the standards and rules for electronic payments, including direct deposit, bill payments, and other bank-to-bank transfers.

ODFI (Originating Depository Financial Institution): The ODFI is the financial institution that initiates ACH transactions on behalf of the originator (the person or business sending the funds). It submits the transaction into the ACH network and is responsible for ensuring compliance with NACHA rules.

Example: If a company pays employees via direct deposit, its bank is the ODFI

RDFI (Receiving Depository Financial Institution): The RDFI is the financial institution that receives ACH transactions on behalf of the recipient (the person or business getting the funds). It processes incoming ACH entries and credits or debits the receiver's account.

Example: An employee's bank receiving a direct deposit paycheck is the RDFI

Key NACHA Information

NACHA Operating Rules place the responsibility on the ODFI to ensure that the Originator has authorization – Therefore strict liability falls on the ODFI

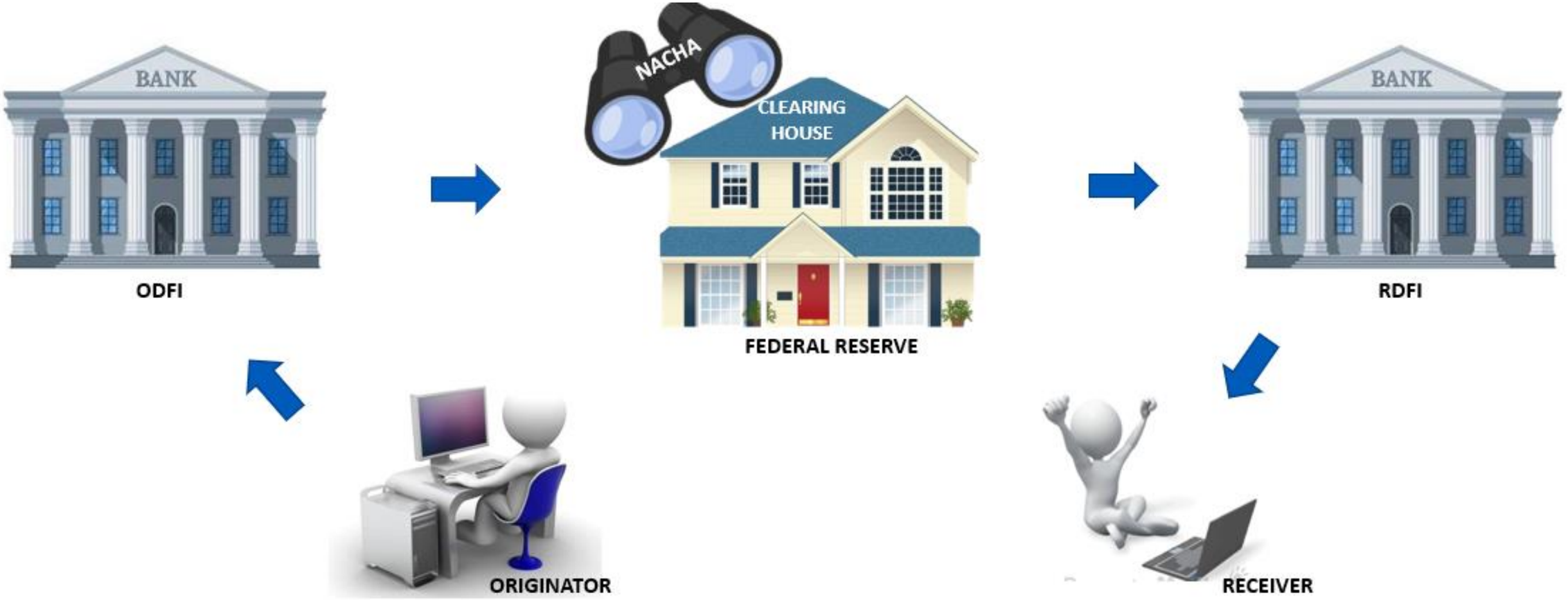
Determining the ODFI is a crucial step when trying to obtain information about an account or account holder tied to an ACH transaction as the the ODFI, Why?

- Primary source of transaction data
- Where the verification & authorization occurs
- How to handle return & dispute handing
- Ensure compliance and oversight rules come into play

**Consumer ACH Transactions are regulated under Regulation E under The Electronic Funds Act

***Business accounts do not fall under Regulation E, but do fall under the NACHA Operating Rules solely

ACH Workflow



ACH Basics - Zelle



Zelle is a digital payment network that enables fast, direct transfers between U.S. bank accounts using only an email address or mobile number

Key Features:

- Instant Transfers: Funds typically arrive within minutes.
- Bank-Integrated: Built into the apps of most major U.S. banks and credit unions.
- No Fees: Zelle doesn’t charge users for sending or receiving money.
- Simple User Experience: No need for bank account numbers.

ACH Basics - Zelle

Common Uses:

- Paying friends or family
- Splitting rent or utilities
- Reimbursing coworkers or teammates



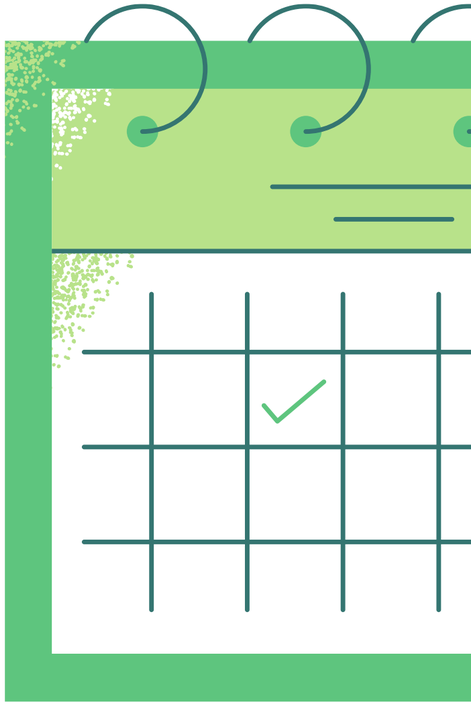
Security Considerations:

- No fraud protection for goods/services – only use with trusted individuals.
- Transactions are final – not easily reversed.
- New liability Shift rules in place as of June 31, 2023

Despite the immediate availability of funds, the actual settlement takes place over the normal ACH cycle. Therefore, the originating bank assumes the liability.

ACH Basics - Zelle

Types of Zelle Fraud



Impersonation Scams

- Fraudsters pose as bank representatives, family members, or utility companies.
- Victims are tricked into sending money via Zelle under false pretenses.

Phishing Attacks

- Fake emails, texts, or calls direct users to bogus websites or prompt them to “verify” credentials.
- Criminals use this information to access Zelle accounts and transfer funds.

Romance Scams

- Scammers build online relationships and eventually request money through Zelle for emergencies, travel, or medical expenses.

ACH Basics - Zelle

Types of Zelle Fraud

Marketplace Scams

- Fraudsters post fake items for sale (e.g., tickets, electronics).
- Once paid via Zelle, they disappear—no product is delivered.

Account Takeover Fraud

- Criminals gain access to a victim's online banking and use Zelle to transfer funds.
- Often the result of weak passwords or stolen credentials.

Business Email Compromise (BEC)

- Targeting companies: fake invoices or payment requests direct business users to pay "vendors" via Zelle.



WIRE TRANSACTION BASICS

Wire Fraud Red Flags & Risks

Urgent or Last-Minute Requests

- Requests to send funds immediately, especially involving changes to payment instructions.

Changes to Known Payment Information

- Sudden updates to bank account details via email—especially from a vendor or executive.

Unusual Language or Grammar

- Poorly worded emails or messages that don’t match the sender’s typical tone.

Suspicious Email Addresses

- Slight variations in domain names (e.g., @abccompany.com vs. @abccornpany.com).

Wire Fraud Red Flags & Risks

Requests to Bypass Standard Procedures

- Pressure to skip verification steps, such as dual approvals or call-back confirmations.

Unfamiliar Beneficiary Names or Banks

- Transfer requests to new accounts or foreign banks without prior notice.

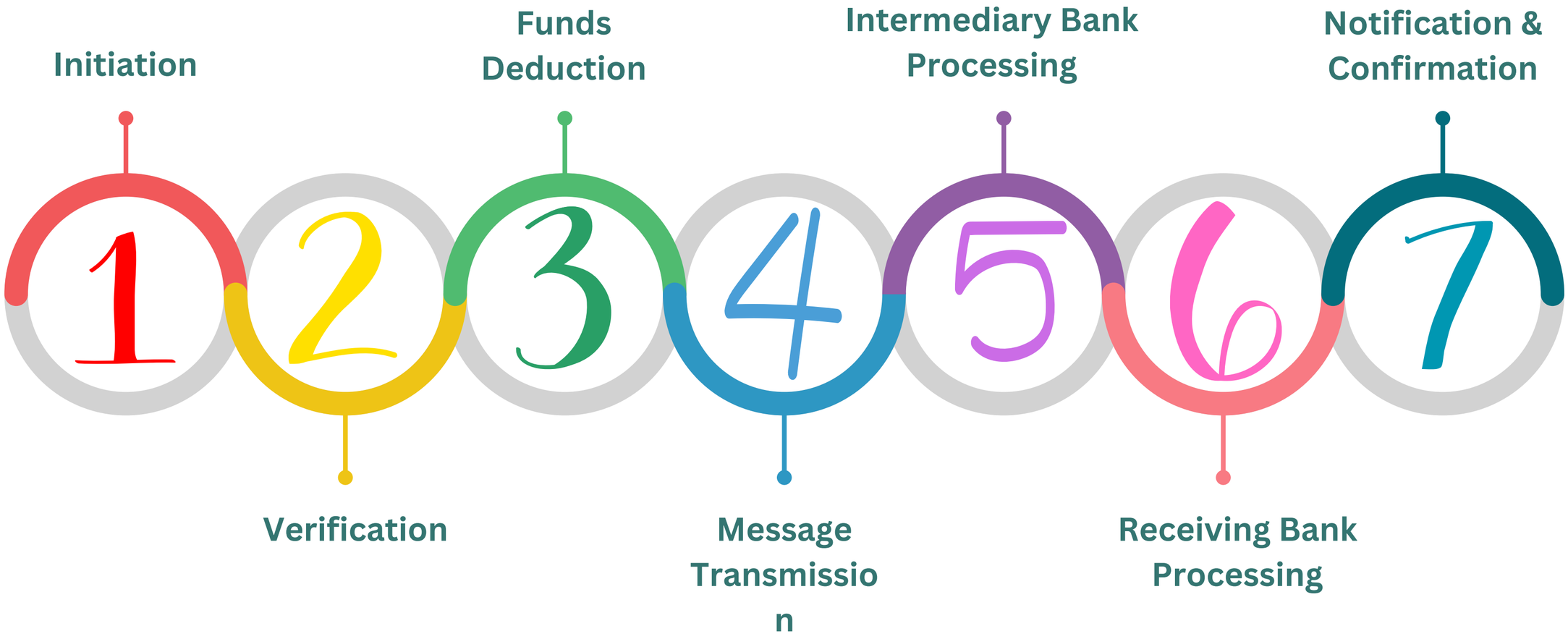
No Phone Verification

- Wire instructions sent without a voice-confirmed callback to a known contact number.

International Destinations with No Business Justification

- Wires to countries not previously involved in the transaction or business relationship.

Wire Transaction Basics



Wire Transactions

FBI – financial fraud Kill Chain (FFKC)

This is another avenue that financial institutions can use to potentially recover funds for victims of wire fraud

The wire(s) must meet the following criteria:

- The wire is $50,000.00 or above
- The wire is international
- A SWIFT recall notice has been initiated
- The wire has occurred within the last 72 hours

To initiate the FFKC, banks contact the local FBI field office and provide all of the wire information



ACH Key Terms Defined

Originator

- The person or entity sending the wire transfer.

Beneficiary

- The person or entity receiving the wire transfer.

Intermediary Bank

- A bank that facilitates the transfer between the originating and receiving banks, often used in international wires.

SWIFT Code

- A unique identifier for banks in international wire transfers; also known as a BIC (Bank Identifier Code).

Routing Number (ABA Number)

- A 9-digit code identifying U.S. financial institutions, used in domestic wires.

BAN (International Bank Account Number)

- Used in many countries outside the U.S. to identify specific bank accounts for international transfers.

Key NACHA Information

Fedwire

- The real-time gross settlement system used by U.S. banks for domestic wire transfers via the Federal Reserve.

CHIPS (Clearing House Interbank Payments System)

- A private-sector U.S. clearing system for large-value domestic and international dollar payments.

Wire Transfer Number

- A unique reference or confirmation number assigned to each wire transfer.

OFAC Screening

- Office of Foreign Assets Control screening required for wire transactions to ensure compliance with U.S. sanctions laws

ONLINE BANKING BASICS

Online Banking Basics

Online banking/Bill Pay is another channel where account holders manage their account and issue payment instructions to various merchants or individuals

Online Banking is also susceptible to account takeovers, which enables the fraudster to access the customer account and initiate services such as:

- change addresses
- order debit cards
- change PINs
- order checks
- initiate ACH
- Initiate bill payments

Account Takeover is typically perpetrated by:

- Scams in which the customer provides OLB login credentials
- Phishing
- Malware
- Identity Theft



Online Banking Basics

When a customer falls victim to a scam in which they provide their OLB credentials to the fraudster, this permission can affect the customer's entire relationship to include lines of credit such as HELOC's and savings such as IRA's.

A common scam is the customer provides the fraudster with their debit card and OLB credentials

- The fraudster then logs in to the customer account and transfers funds from lines of credit and savings into the account which is accessible by the debit card or bill pay
- Funds can also be withdrawn via ATM withdrawals and POS transactions.



Online Banking Basics

ID Theft in opening online accounts provides an avenue for moving illicit funds using multiple fraud types – Wire, ACH, and check fraud or a combination

The data available to assist in investigations includes:

- IP address
- IP Type and Provider
- device info such as device type and browser used
- a log of user activity with dates, times, and user ID
- Some banks also capture geo data.



ATM/DEBIT CARD BASICS



ATM/Debit Card Basics

ATM and debit cards provide account holders with direct access to their funds. They can be used to withdraw cash from ATMs or to make purchases at merchants for goods and services. Like any other method of accessing bank funds, ATM and debit card fraud is a common risk and can result in unauthorized withdrawals or transactions.

- **Skimming** - Devices installed on ATMs or gas pumps capture card data and PINs
- **Card Cloning** - Information from a skimmed card is used to create a duplicate card for fraudulent transactions
- **Card Trapping** - Fraudsters install devices that trap a user's card in the ATM and later retrieve it
- **Shoulder Surfing & PIN Theft** - Criminals observe users entering their PINs or use hidden cameras to capture key presses
- **Lost or Stolen Cards** - Thieves use found or stolen cards to make purchases or ATM withdrawals before the card is reported.
- **Fake ATMs** - Entire machines or overlays built to look real are used to steal card data and PINs.
- **Account Takeover** - Fraudsters gain access to a victim's bank account and order a replacement debit card mailed to a new address

ATM/Debit Card Basics - Card Cracking

A TYPICAL CARD CRACKING SCENARIO

1. A fraudster sends you a social media message to "make quick cash"

IF U WANT 2 MAKE REAL LEGIT MONEY NO SCAM IF U HAVE A BANK ACCOUNT HMU

2. Enticed by the promise of money, **YOU** provide the scammer a debit card, PIN or online credentials—giving them direct access to account

1234 5678 9012 3456

PIN

3. The fraudster deposits a fake check in your account



4. Money is withdrawn immediately at an ATM



5. The fraudster gives the account holder a kickback



6. **YOU** call the bank to report a lost or stolen card, or compromised credentials



7. Bank reimburses the stolen funds to **YOU**

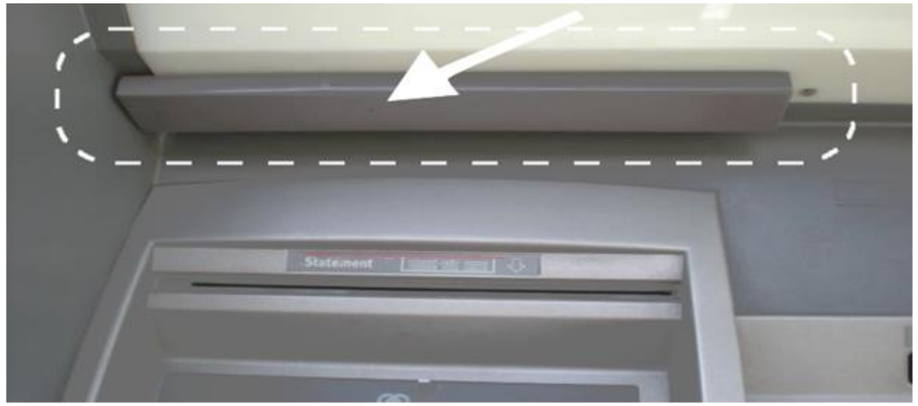


8. **YOU** are now a **CRIMINAL ACCOMPLICE**



ATM/Debit Card Basics - Skimming

Traditional skimmers are made to look like ATM components and are attached to the fascia



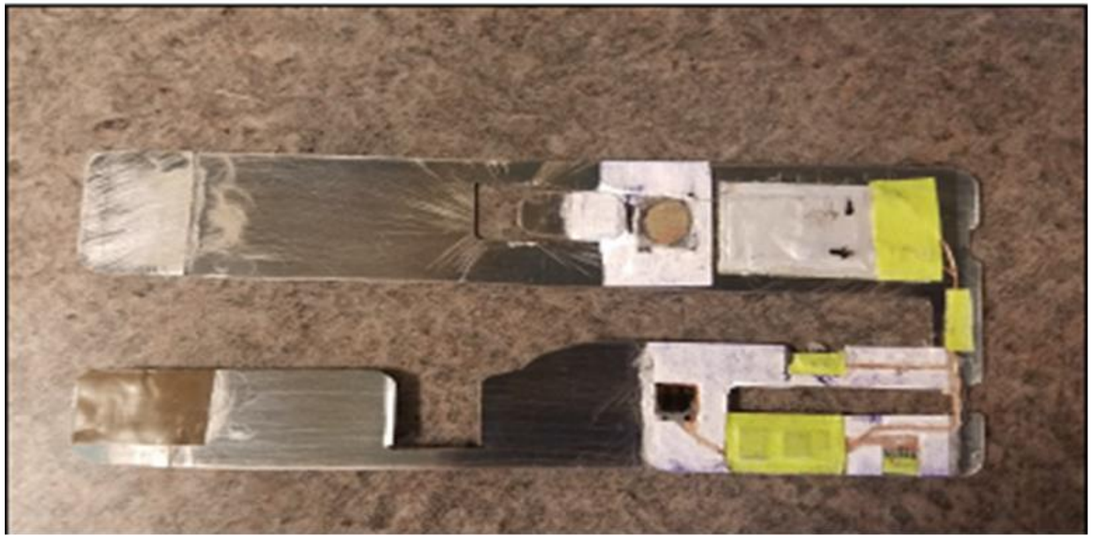


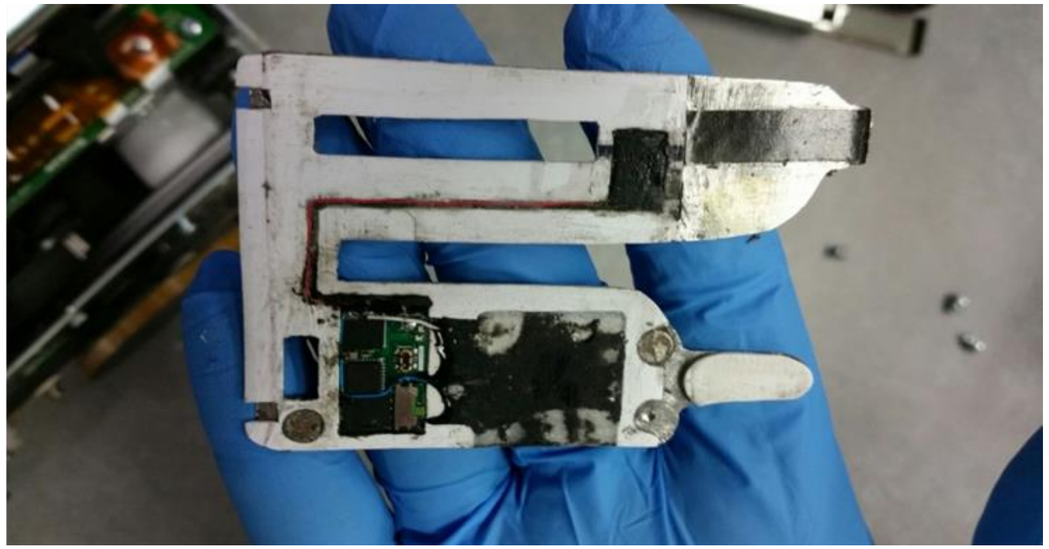




ATM/Debit Card Basics - Skimming

Deep insert skimmers are inserted into the card reader and can go unnoticed in the absence of anti-skimming devices





BANKING REGULATIONS

Regulation E – The Electronic Funds Act

The Electronic Funds Act was passed in 1978 to its aimed to protect the rights of consumers when they engage in electronic transactions. The Federal Reserve Implements the EFT Act through Regulation E: 12 CFR 205



Regulation E provides a basic framework that establishes the rights, liabilities, and responsibilities of participants in electronic fund transfer systems such as automated teller machine transfers, telephone bill-payment services, point-of-sale (POS) terminal transfers in stores, and preauthorized transfers from or to a consumer's account (such as direct deposit and social security payments). The term "electronic fund transfer" (EFT) generally refers to a transaction initiated through an electronic terminal, telephone, computer, or magnetic tape that instructs a financial institution either to credit or to debit a consumer's asset account.

Regulation E – The Electronic Funds Act

Important Guidelines for Reporting Fraudulent Transactions

- When fraud occurs on a bank account, it is the client's responsibility to report any fraudulent transactions promptly, in accordance with the bank's Deposit Agreement and Regulation E.

- Unauthorized or fraudulent Electronic Funds Transfer (EFT) transactions involving consumer clients must be assessed by the bank, following the directives of Regulation E.

- Clients can report EFT fraud by notifying the bank either in writing or verbally.

- Banks have specific timeframes to resolve client claims, which is set at 10 business days.

Regulation E – The Electronic Funds Act

Important Guidelines for Reporting Fraudulent Transactions - Cont.

- If the bank requires additional time, they may issue provisional credit (within the 10 business days, provided that the bank has a signed dispute form) and continue with the investigation.

- The bank cannot mandate that clients report the fraud to law enforcement.

Clients may be held accountable for any losses incurred due to late notification of errors or fraud.



Bank Regulations - CFPB

Regulation C [Home Mortgage Disclosure Act (HMDA)]
Regulation D [Alternative Mortgage Transaction Parity]
Regulation E [Electronic Funds Transfer Act (EFT)]
Regulation F [Fair Debt Collection Practices Act (FDCPA)]
Regulation G [S.A.F.E. Act & Residential Mortgage Loan Originators]
Regulation H [S.A.F.E. Act - State Compliance & Bureau Registration System]
Regulation I [Disclosure Requirements - Depository Institutions Lacking FDIC Insurance]
Regulation J [Land Registration]
Regulation K [Purchasers' Revocation Rights, Sales Practices and Standards]
Regulation L [Special Rules of Practice]

cfpb Consumer Financia Protection Bureau

Bank Regulations - CFPB

Regulation L [Special Rules of Practice]
Regulation M [Consumer Leasing]
Regulation N [Mortgage Acts and Practices - Advertising]
Regulation O [Mortgage Assistance Relief Services]
Regulation P [Privacy of Consumer Financial Information]
Regulation V [Fair Credit Reporting (FCRA)]
Regulation X [Real Estate Settlement Procedures Act (RESPA)]
Regulation Z [Truth in Lending Act (TILA)]
Regulation DD [Truth in Saving Act (TISA)]
Unfair, Deceptive, or Abusive Acts or Practices (UDAAP Exam Manual)



Bank Regulations - FDIC

FDIC Laws, Regulations, & Related Acts
FDIC Financial Institution Letters (FILs)
FDIC Compliance Exam Manual
Part 1000 Section 20 - Participation in Lotteries and Related Activities
Part 323 - Appraisals
Part 326 - Minimum Security Devices and Procedures and Bank Secrecy Act Compliance
Part 328 - Advertisement of Membership
Part 337 - Unsafe and Unsound Banking Practices

FDIC
FEDERAL DEPOSIT INSURANCE CORPORATION

Bank Regulations - FDIC

- Part 339 - Loans in Areas Having Special Flood Hazards
- Part 343 - Consumer Protection in Sales of Insurance
- Part 345 - Community Reinvestment
- Part 362 - Activities of Insured State Banks and Insured Savings Associations
- Part 363 - Annual Independent Audits and Reporting Requirements
- Part 364 - Standards for Safety and Soundness
- Part 365 - Real Estate Lending Standards

FDIC
FEDERAL DEPOSIT INSURANCE CORPORATION

Bank Regulations - FDIC



The privacy rule governs when and how banks may share nonpublic personal information about consumers with nonaffiliated third parties.

FDIC
FEDERAL DEPOSIT INSURANCE CORPORATION

Bank Regulations - FFIEC

HMDA Tools
IT Exam Handbook Infobase
BSA/AML Infobase



FFIEC
Federal Financial Institutions Examination Council

Bank Regulations - US Dept. of Treasury

FinCEN Advisories, Bulletins, & Fact Sheets
FinCEN Statutes & Regulations
OFAC
General Provisions

Bank Regulations - FTC

E-Sign Act
Fair Credit Reporting Act (FCRA)
Fair Debt Collection Protection Act (FDCPA)

Bank Regulations - OCC

OCC Bulletins
OCC Comptroller's Handbook
Sales of Credit Life Insurance
Consumer Protection in Sales of Insurance
Minimum Security Devices and Procedures, SAR & BSA Compliance Program
Loans in Areas having Special Flood Hazards
Community Reinvestment Act (CRA)
Lending Limits
Real Estate Lending and Appraisals

Bank Regulations - FRB



- Federal Reserve Regulations Listing
- Federal Reserve Supervision Manuals
- Regulation A [Extensions of Credit By Federal Reserve Banks]
- Regulation D [Reserve Requirements of Depository Institutions]
- Regulation F [Limitations on Interbank Liabilities]
- Regulation G [Disclosure and Reporting of CRE-Related Agreements]
- Regulation H [Membership of State Banking Institutions in the Federal Reserve System]
- Regulation I [Issue and Cancellation of Federal Reserve Bank Capital Stock]
- Regulation J [Collection of Checks/Other Items by FRB Banks & Fund Transfers by Fedwire]
- Regulation K [International Banking Operations]
- Regulation L [Management Official Interlocks]
- Regulation O [Loans to Executive Officers, Directors and Principal Shareholders of Banks]
- Regulation R [Exceptions for Banks from the Definition of Broker]
- Regulation S [Reimbursement for Providing Financial Records; Recordkeeping Requirements]
- Regulation U [Credit by Bankers - Purchasing or Carrying Margin Stock]
- Regulation W [Transactions Between Member Banks and Their Affiliates]
- Regulation X [Borrowers of Securities Credit]
- Regulation Y [Bank Holding Companies and Change in Bank Control]

Bank Regulations - FRB

- Regulation W [Transactions Between Member Banks and Their Affiliates]
- Regulation X [Borrowers of Securities Credit]
- Regulation Y [Bank Holding Companies and Change in Bank Control]
- Regulation BB [Community Reinvestment Act (CRA)]
- Regulation CC [Availability of Funds and Collection of Checks]
- Regulation FF [Obtaining and Using Medical Information in Connection with Credit]
- Regulation GG [Prohibition on Funding of Unlawful Internet Gambling]
- Regulation II [Debit Card Interchange Fees and Routing]
- Regulation LL [Savings and Loan Holding Companies]
- Regulation MM [Mutual Holding Companies]
- Regulation PP [Definitions Relating to Title I of the Dodd-Frank Act]
- Regulation QQ [Resolution Plans]
- Regulation RR [Credit Risk Retention]
- Regulation TT [Supervision and Regulation Assessments of Fees]
- Regulation WW [Liquidity Risk Measurement Standards]
- Regulation XX [Concentration Limit]
- Regulation YY [Enhanced Prudential Standards]



Resources

- Board of Governors of the Federal Reserve System - https://www.federalreserve.gov/
- The Federal Reserve System - https://federalreserveonline.org/
- The Basic Structure of the Uniform Commercial Code - https://www.stimmel-law.com/en/articles/uniform-commercial-code-basic-structure
- NACHA Operating Rules (ACH Transactions) - https://www.nacha.org/rules/operating-rules
- FBI’s Internet Crime Complaint Center (IC3) - https://www.ic3.gov/
- Consumer Financial Protection Bureau (CFPB) - https://www.consumerfinance.gov/compliance/supervision-examinations/
- Federal Deposit Insurance Corporation (FDIC) - https://www.fdic.gov/
- Federal Financial Institutions Examinations Council (FFIEC) - https://www.ffiec.gov/
- Federal Trade Commission (FTC) - https://www.ftc.gov/
- Office of the Comptroller of the Currency (OCC) - https://www.occ.treas.gov/topics/supervision-and-examination/examinations/examinations-overview/index-examinations-overview.html
- U.S. Department of the Treasury - https://www.treasury.gov/about/organizational-structure/offices/Pages/bfs.aspx


THANK YOU!

John Fick, MLS, CFE, CFCI, CECFE

Director of Fraud
Northwest Bank

John.Fick@Northwest.com
Johnfick@info.com
469.400.2885

SCAN ME