

FRAUD ON YOUR FINANCE DEPARTMENT:

Risks, Rules and Recommendations for Preventing Bank Account Frauds

Follow us on social media!





@delvacca

Presenters:



Jean Day, Senior Counsel – Litigation, TD Bank, N.A.



Christopher J. Tucci, Senior Counsel – Litigation, PNC Financial Services Group, Inc.



Alexander D. Bono, Partner, Duane Morris LLP



Ryan E. Borneman, Partner, Duane Morris LLP



Lynne E. Evans, Associate, Duane Morris LLP





Fraud Is Big Business

There has been a <u>significant increase</u> in fraud attacks on companies, with:

- 78% of companies experiencing actual/attempted payments fraud in 2017, a 4% increase from 2016 and the largest percentage on record.
- 74% of companies reported experiencing check fraud (the payment method most often targeted).
- 28% of companies reported experiencing ACH debit fraud, and 13% experiencing ACH credit fraud.
- 77% of companies reported experiencing **Business Email Compromise (BEC)**, with 54% of BEC scams **targeting wire transfers**.

Source: Association For Financial Professionals, 2018 AFP Payments Fraud and Control Survey (2018).





Fraud Is A Big Cost

- 92% of companies reported that fraud attacks cost their companies half a percent of total revenue.
- FBI tracked losses of *\$5.3 billion* from *Business Email Compromise / Email Account Compromise* for three year period ending December 2016.
- Costs include direct money losses from payments fraud, high clean up costs following fraud incidents, and costs of investing in and implementing fraud prevention measures.
- Consumers reported losing nearly \$1.48 billion to fraud in 2018, arising out of over 1.4 million fraud reports, with wire transfers continuing to be the most frequently reported payment method for fraud.

Sources: Federal Trade Commission, Consumer Sentinel Network Data Book for 2018 (2019); Association For Financial Professionals, 2018 AFP Payments Fraud and Control Survey (2018).





Payments Fraud Roadmap

- 1. Check Fraud
- 2. ACH Fraud
- 3. Wire Fraud
- 4. Electronic Fund Transfer (EFT) Fraud
- 5. Credit Card Fraud





CHECK FRAUD

Check Fraud: Forged Maker

"A bank may charge against the account of a customer an item that is *properly payable* from that account even though the charge creates an overdraft. An item is properly payable *if it is authorized by the customer* and is in accordance with any agreement between the customer and bank."

UCC § 4-401





Check Fraud: Forged Maker – Defenses

If bank "makes available" account statements showing check, amount and date of payment, then "customer must exercise reasonable promptness in examining the statement". UCC § 4-406

Three Defenses:

- 1. Repeater Rule: Customer barred from recovery of fraud committed by the same wrongdoer if customer failed to notify bank of fraud within 30 days of bank statement showing first fraud, unless bank did not exercise ordinary care. UCC § 4-406(d)
- 2. One Year Rule: Customer barred from recovery "without regard to care or lack of care" if customer failed to notify bank within 1 year of statement. UCC § 4-406(f)
- 3. Statute of Limitations: Three years. UCC § 3-118





Check Fraud: Forged Endorsements

"A bank may charge against the account of a customer an item that is *properly payable* from that account even though the charge creates an overdraft. An item is properly payable *if it is authorized by the customer* and is in accordance with any agreement between the customer and bank."

UCC § 4-401





Check Fraud: Forged Endorsements – Warranties

Presentment Warranties: A depositor bank that "presents" a check to a drawee bank for payment warrants:

- (a) The warrantor is, or was, at the time the warrantor transferred the draft, a person entitled to enforce the draft or authorized to obtain payment or acceptance of the draft on behalf of a person entitled to enforce the draft;
- (b) The draft has not been altered; and
- (c) The warrantor has no knowledge that the signature of the drawer of the draft is unauthorized.

UCC § 3-417





Check Fraud: Forged Endorsements – Warranties

Transfer Warranties: A depositor bank that "transfers" a check to a drawee bank for payment warrants:

- (a) The warrantor is a person *entitled to enforce the instrument*;
- (b) All signatures on the instrument are authentic and authorized;
- (c) The instrument has not been altered;
- (d) The instrument is not subject to a defense or claim in recoupment of any party which can be asserted against the warrantor; and
- (e) The warrantor has no knowledge of any insolvency proceeding commenced with respect to the maker or acceptor or, in the case of an unaccepted draft, the drawer.

UCC § 3-416





Check Fraud: Forged Endorsements - Defenses

- Payee Received Effective Benefit: No right to recover if payee received benefit of funds, *i.e.*, converted to property payee received.
- Check Deposited with Intended Payee: The proper payee is determined by the intent of the drawer, even if drawer is the fraudster.
- Local adaptation: Florida: one-year includes fraudulent endorsements
- Statute of Limitations: Three years. UCC § 3-118





Check Fraud: Typical Bank Account Agreement

Forged items: Your statement is considered correct, and we will not be liable for payments made and charged to your account unless you notify us of an error or other irregularity, including unauthorized payment, within 30 calendar days of the delivery date of the earliest statement describing the charge or deposit to your account.





Check Fraud: Real World Examples

- 1. Rogue Bookkeeper diverted company checks
- 2. Unidentified Fraudsters transferred funds (via EFT and remotely created checks) to various retail entities to pay bills and other charges not incurred by accountholder
- 3. **Unauthorized Employees** moved money between various business accounts without authorization and contrary to company's internal controls





Check Fraud: Recommendations for Check Fraud Prevention

- Know applicable time limits for reviewing and reporting suspected fraud (under account agreement(s) and UCC);
- 2. Promptly *review bank statements* and check images (if available), and notify bank of unauthorized payments;
- 3. Make sure that there is **oversight of employees** with bookkeeping / accounting functions, access to signature stamp, etc.;
- 4. Segregate duties to improve internal accounting controls;
- 5. Require *two signers* for checks over certain threshold.







ACH FRAUD

ACH Fraud: Background

ACH Originator – initiates ACH transaction;

Originating Depository Financial Institution (ODFI) – receives payment instructions from ACH Originator;

ACH Operator - central clearing facility that processes ACH transactions;

Receiving Depository Financial Institution (RDFI) – receives ACH transaction and credits or debits Receiver's account;

ACH Receiver – authorizes ACH transaction, either as a debit or credit to Receiver's account.

Source: FFIEC, Bank Secrecy Act Anti-Money Laundering Examination Manual, Automated Clearing House Transactions – Overview.





ACH Fraud: ACH Background

Two Types of Transactions -

Direct Deposit via ACH – e.g., payroll, employee expense reimbursement, government benefits, tax and other refunds, and annuities and interest payments;

Direct Payment via ACH -

- ACH credit transaction company (Originator) sends money to Receiver's account;
- ACH debit transaction money transferred from Receiver's account to company (Originator);

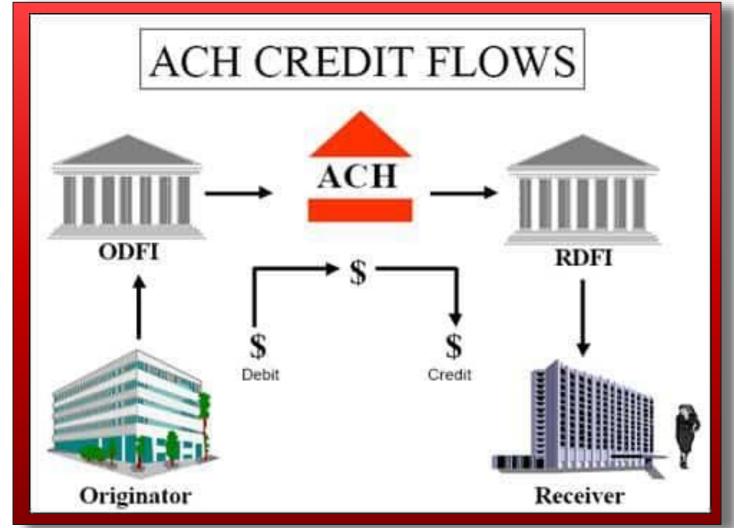
NACHA Rules require that ACH credits settle in 1-2 business days and ACH debits settle on next business day;

Source: nacha.org, "What is ACH?: Quick Facts About the Automated Clearing House (ACH) Network".





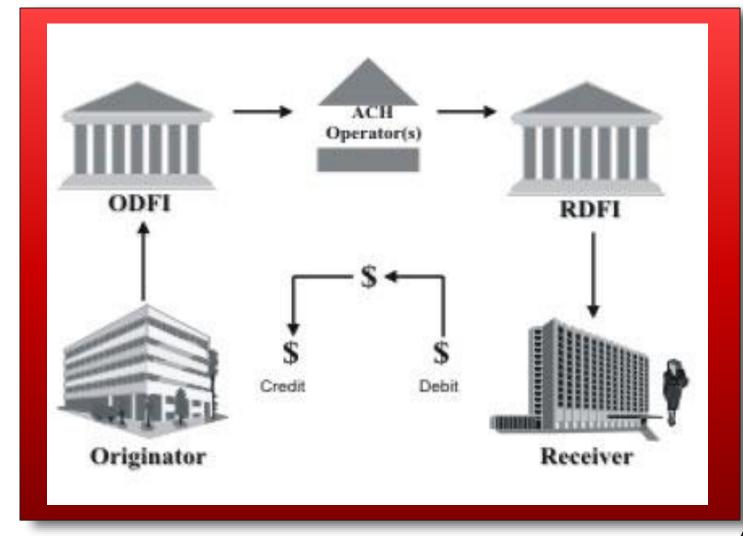
Funds Flow for ACH Credit Transaction





Association of Corporate Counsel

Funds Flow for ACH Debit Transaction





Source: OCC Bulletin 2006-39, Automated Clearing House Activities (Sept. 1, 2006).

Association of Corporate Counsel

ACH Fraud: Rules

NACHA manages development, administration and governance of ACH Network;

ACH transactions are covered by:

- NACHA Operating Rules and Operating Guidelines (collectively, "NACHA Rules");
- UCC Article 4A (for corporate transactions only);
- EFTA/Reg E (for consumer transactions only);
- Bank account agreements.

Source: nacha.org, "What is ACH?: Quick Facts About the Automated Clearing House (ACH) Network".





ACH Fraud: Obligations of ODFI

NACHA Rules place responsibility on ODFI to ensure that ACH transfers are properly authorized;

- *ODFI* is "*responsible for all Entries* originated through the ODFI". *NACHA Rule* 2.1;
- Originator "must obtain authorization from the Receiver to originate one or more Entries to the Receiver's account." NACHA Rule 2.3.1;
- *ODFI "warrants"* to RDFI that *transaction "has been properly authorized* by the Originator [customer] and the Receiver". *NACHA Rule* 2.4.1.1;
- ODFI "shall indemnify" RDFI from and against any and all claims resulting from "breach of any warranty made to such party by the ODFI" or "the debiting or crediting of an Entry to a Receiver's account in accordance with the terms of the Entry". NACHA Rule 2.4.5.1.





ACH Fraud: Obligations of RDFI

- RDFI "must accept" ACH transfers. NACHA Rule 3.1.1.
- RDFI "may rely solely on the account number". NACHA Rule 3.1.2.
- RDFI "must make the amount of the credit Entry received . . . available to the Receiver [customer] for withdrawal no later than the end of the Settlement Date of the Entry." NACHA Rule 3.3.1.





ACH Fraud: Obligations of ACH Originator (UCC Article 4A)

A *payment order* (ACH transfer) *is effective* as the order of the customer, whether or not authorized, *if it is verified pursuant to a security procedure*. *UCC 4A-202(b);*

A "**Security procedure**" is "a procedure established by agreement of a customer and a receiving bank for the purpose of . . . verifying that a payment order . . . is that of the customer[.]" UCC 4A-201;

The effect of UCC 4A-202(b) is to "place the risk of loss on the customer" where a payment order, even if unauthorized by the customer, is verified by a commercially reasonable security procedure. UCC 4A-203, Official Cmt. 5.





ACH Fraud: Obligations of ACH Originator (Typical Account Agreement)

Customer (ACH Originator) must indemnify ODFI against any claim for a refund by a consumer or corporate Receiver;

Customer must comply with security procedures, and agrees that they are a commercially reasonable method for verifying authenticity of entries;

Customer is strictly responsible for establishing, implementing, maintaining and updating its own security procedures to safeguard against unauthorized transmissions, and relating to initiation, processing and storage of ACH entries;

If an entry purports to have been transmitted or authorized by Customer, it will be deemed effective and Customer shall be obligated to pay ODFI the amount of such entry, even if not authorized, provided ODFI acted in compliance with security procedures;

Customer shall have no right to cancel or amend any entry or file after its receipt by ODFI (ODFI may request cancellation of entry prior to transmitting it to ACH Operator, but shall have no liability if cancellation is not effected);

Customer warrants that every entry sent to ODFI is authorized by Receiver;





ACH Fraud: Real World Examples

- Rogue Employee embezzled millions from employer through fraudulent ACH scam
- 2. Organized Crime Group caused over \$724k to be transferred from online IRA account to bank via ACH, and then funds transferred overseas







GREATER PHILADELPHIA

ACH Fraud: Recommendations for ACH Fraud Prevention

- Segregate duties / Do not vest complete control over ACH (or any other transaction) in single employee, without oversight;
- Implement dual controls / dual approval procedures;
- Implement Positive Pay or other security features;
- Implement call back procedures;
- Use token creating random code to be used in conjunction with user ID and PIN;
- Limit ACH transaction rights to select employees;
- Monitor accounts online daily timing is absolutely essential for trying to recoup funds from fraudulent debits from Originator's account;
- Perform regular reconciliations;
- Implement email / computer security measures (discussed in wire transfer section below).





WIRE FRAUD

Wire Fraud: UCC Article 4A

UCC Article 4A (Funds Transfers)

- Applies to business/commercial wire transfers
- Does not apply to consumer wire transfers (which are instead governed by EFTA)

"Security procedure" – procedure established by agreement between customer and receiving bank for purpose of:

- verifying that a payment order is that of the customer, or
- detecting error in the transmission or the content of the payment order or communication.

UCC § 4A-201





Wire Fraud: UCC Article 4A

A *payment order* (wire transfer) *is effective* as the order of the customer, whether or not authorized, *if it is verified pursuant to a security procedure*. *UCC 4A-202(b)*.

The effect of UCC 4A-202(b) is to "place the risk of loss on the customer" where a payment order, even if unauthorized by the customer, is verified by a commercially reasonable security procedure. UCC 4A-203, Official Cmt. 5.

Receiving bank is not entitled to enforce or retain verified payment order if customer proves the order was not caused by a person –

- Entrusted to act for customer with respect to payment orders or security procedure, or
- Who obtained access to customer's transmitting facilities or information facilitating breach of security procedure.

UCC 4A-203.





Wire Fraud: Unauthorized Payment Orders

Receiving bank must *refund* payment of a payment order, and pay interest on the refundable amount, if it accepts a payment order issued in the name of its customer as sender which is:

- Not an authorized and/or verified payment order of the customer (pursuant to Section 4A-202), or
- Not an enforceable verified payment order (pursuant to Section 4A-203).

UCC 4A-204





Wire Fraud: Phishing / Spear-Phishing Threats

- **Phishing** email appears to come from credible entity (e.g., bank or employer), but a scam designed to dupe victim into turning over confidential information or clicking on malicious link;
- Spear-Phishing phishing involving highly detailed information about recipient and/or people they know in much more targeted attack;
- 38% of firms polled in U.S. and UK in 2016 reported that cyberattacks they suffered were
 the results of spear-phishing campaigns;
- Average phishing attack cost a mid-sized company nearly \$1.6 million to remedy;
- Phishing attempts grew by 65% between 2016-2017.

Source: Joel Griffin, "Hackers refine, improve their phishing skills" (Feb. 8, 2019).





Wire Fraud: Real World Examples

- Saudi Prince company subject to spear-phishing attack and wired \$1M to account, then drained
- 2. Cyber Fraud on Law Firm





Wire Fraud: Recommendations for Wire Fraud Prevention

- Same recommendations as for ACH transactions;
- Emails / computer systems are particularly likely methods for attack, so educate employees and ensure computer controls are in place;
- Be wary of any email requesting security credentials;
- Ensure all computer equipment is regularly updated and patched for security vulnerabilities;
- Ensure all user IDs, passwords, authentication methods and other security procedures are protected and kept confidential;
- Educate all employees about risky emails / phishing attacks and computer use;
- Educate all employees about reporting procedures for suspicious activity.





EFT FRAUD

EFT Fraud: EFTA / Reg E

Electronic Fund Transfer Act ("*EFTA*"), 15 U.S.C. §§ 1693, *et seq.*, aims to protect individual consumers engaging in electronic fund transfers ("*EFT*") and remittance transfers.

Implemented through Regulation E, 12 CFR 1005, et seq.

EFT services include:

- Transfers through automated teller machines (ATMs),
- Point-of-sale (POS) terminals,
- Automated clearinghouse (ACH) systems,
- Telephone bill-payment plans in which periodic or recurring transfers are contemplated,
- Remote banking programs, and
- Remittance transfers (Subpart B).





EFT Fraud: Unauthorized EFTs

"Unauthorized" EFT is a transfer from a consumer's account initiated by a person other than the consumer without authority to do so, and from which the consumer receives no benefit. 12 CFR 1005.2(m)

Consumer liability for unauthorized EFTs:

- Determined solely by consumer's promptness in notifying the financial institution
- Bank may not use other factors as basis to hold consumers liable 12 CFR 1005.6







CREDIT CARD

Credit Card Fraud: TILA / Regulation Z

Truth In Lending Act, 15 U.S.C. §§ 1601, et seq. ("TILA") aims to –

- protect consumers from liability for charges resulting from the unauthorized use of their credit cards;
- require creditors to investigate and promptly correct billing errors; and
- allow consumers to maintain against a creditor much the same claims they can assert against a merchant in connection with the purchase of defective or unsatisfactory goods and services.

Implemented by **Regulation Z**, 12 CFR 226, et seq.





Credit Card Fraud: Liability of Cardholder

"Unauthorized use" means the use of a credit card

- by a person, other than the cardholder, who does not have actual, implied, or apparent authority for such use, and
- from which the cardholder receives no benefit.

Cardholder must notify card issuer of pertinent information about the loss, theft or unauthorized use of a credit card

Notification may be given in person, by telephone or in writing





Credit Card Fraud: Liability of Cardholder

Cardholder's liability for unauthorized use -

Shall not exceed the lesser of \$50 or the amount of money, property, labor, or services
obtained by the unauthorized use before notification to the card issuer

12 CFR 226.12(b)(1)(ii)

If dispute not satisfactorily resolved, then the cardholder may also

- assert against card issuer all claims (other than tort claims) and defenses;
- withhold payment up to the amount of credit outstanding for the property or services that gave rise to the dispute (and card issuer shall not report that amount as delinquent until settled or judgment rendered).

12 CFR 226.12(c)





THANK YOU!

April 24, 2019





A reminder about the benefits of ACC membership...

- Free CLE, like the one you're attending right now
- Roundtables
- Networking meetings
- Special events
 - Spring Fling, Fall Gala, Diversity Summer Program, Golf Outing, Pro Bono clinics, Charity Softball Game & Family Fun Day, and more!



- Access to ACC resources, including:
 - ACC Newsstand (customizable updates on more than 40 practice area)
 - ACC Docket Magazine
 - InfoPAKs
 - QuickCounsel Guides
- For more information or to refer a new member, see your hosts today or contact Chapter Administrator, Chris Stewart, at ChrisStewart@ACCglobal.com.