Identifying Fraudulent Transactions

M. Elizabeth Fast, Esq.
Spencer Fane LLP
Phone: (800) 526-6529 toll free
efast@spencerfane.com

SpencerFane

Who Is Liable for the Fraud Loss?

- The Bad Guy (thief, cybergang, or other fraudster) is ultimately liable for money stolen, but the Bad Guy can't be found or he has already spent the money.
- Since money can't be obtained from the Bad Guy, which of the other parties involved is liable for the loss? As a general rule, the party that was most negligent should be held liable.
- For public policy reasons, however, laws shift the liability to other parties in certain situations.

Who is Liable for the Fraud Loss (cont.)

• Forged maker's signature on paper check	Institution on which check was drawn
• Forged endorsement on paper check	Institution of first deposit
• Alteration of paper check	Institution of first deposit
• Counterfeit paper check	Institution on which check was drawn
• Remotely created item with no maker's signature	Institution of first deposit
• Unauthorized ACH	Originating Depository Financial Institution

Who is Liable for the Fraud Loss (cont.)

• Debit card fraud – consumer	Reg E protects consumer so consumer's institution generally liable to reimburse consumer
• Debit card fraud – commercial	Reg E doesn't protect commercial depositor so generally depends on who was the most negligent (but Visa/MC contract may impose liability on institution)
• Online fraud – consumer	Reg E protects consumer so consumer's institution generally liable to reimburse consumer
• Online fraud – commercial	Reg E doesn't protect commercial depositor – UCC4A permits institution to shift liability to depositor

Fraudulent Checks

- Fraudulent or counterfeit check is not a valid check
- Cashier's check is direct obligation of the issuing institution – little risk if genuine
- Cashier's check said to be "same as cash" – issuing institution can't stop payment against holder-in-due course
- Problem is that there is no issuing institution if it is a fraudulent cashier's check

Identifying Potential Fraudulent Items

- Selling Goods – Consumer sells goods and receives a cashier's check from the buyer for the sales price. Consumer believes the cashier's check is valid so the consumer gives the goods to the buyer. After the consumer deposits the cashier's check into their account, the cashier's check is later returned as fraudulent.
  - Consumer suffers loss of the goods sold.
  - If you want to find out whether a check is genuine, call the institution on which the check is written. Do **not** use the telephone number provided on the instrument.

Identifying Potential Fraudulent Items (cont.)

- Real Example: Bank (i.e., seller) forecloses on inventory and equipment. Bank hired auctioneer to sell the inventory and equipment at public auction. Auctioneer required cash or cashier's check as payment but gave the highest bidders 3 hours to go get cash or cashier's check. One highest bidder returned with cashier's check to purchase his items. Auctioneer thought cashier's check was valid so allowed bidder to take items. Cashier's check was returned as fraudulent. Bank lost the value of the items sold.

Identifying Potential Fraudulent Items (cont.)

- Excess Purchase Price – Consumer sells goods and receives a cashier's check from buyer in an amount greater than the sales price. Buyer asks the consumer to send the excess amount back to buyer. Consumer believes check is valid and deposits it into the consumer's account. Consumer then sends "excess" amount to buyer.
  - Consumer suffers loss of goods sold plus amount of the "excess" funds sent to the buyer.

Identifying Potential Fraudulent Items (cont.)

- Real Example: Seller sells his boat online for $5,000. Buyer sends a $6,000 cashier's check to seller and asks seller to mail the buyer back $1,000. Buyer will pick up the boat in 2 weeks. Seller sent $1,000 back to buyer and seller spent remaining $5,000. Cashier's check was returned as fraudulent causing a $6,000 overdraft in seller's account. Buyer never came to pick up boat.
  - Ask why buyer would be willing to trust seller, who is a perfect stranger, with the "excess" funds.

Identifying Potential Fraudulent Items (cont.)

- Unexpected Windfall – Consumer receives letter stating they have won the lottery including a cashier's check for the amount allegedly won. The letter instructs the consumer to deposit the cashier's check and then to wire a processing fee to a third party. Consumer believes cashier's check is valid and deposits it into consumer's account. Consumer sends processing fee to third party.
  - Consumer suffers loss in amount of processing fee.

Possible Loss to Depository

- Credit Loss – Reversing deposit may cause customer's account to become overdrawn – your institution may never to be able to collect overdraft from customer
- Reputation Loss – Public relations problem – customer may be upset with your institution because customer believes:
  - Your institution should automatically and instinctively know if check is fraudulent
  - Your institution should have followed better procedures to detect fraudulent check
  - Your institution shouldn't have given credit to customer allowing customer to believe good funds were available
  - Your institution shouldn't be able to reverse credit once it has been given to the customer

Scams Where Consumer Suffers Loss But No Loss to Institution

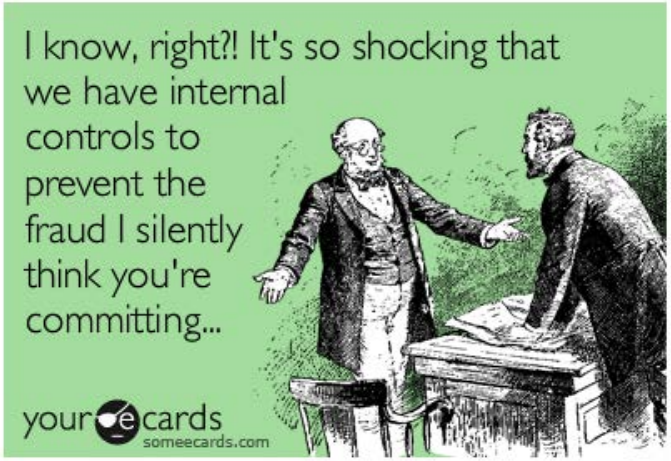
- Abandoned Money - Consumer is told there is $1,000,000 in an account in a foreign country. The $1,000,000 will be wired to the consumer but first the consumer has to pay a foreign transaction fee to get the money out of the foreign country.
  - Consumer suffers loss in the amount of the “foreign transaction fee” that the consumer pays but no loss to institution

Scams Where Consumer Suffers Loss (cont.)

- Grandchild or Friend Needs Money in Foreign Country - Consumer contacted by the U.S. Embassy claiming grandchild or friend is in a foreign country. Their passport and all their money was stolen. Consumer needs to wire funds to foreign country so grandchild or friend can come home.
  - Consumer suffers loss in the amount of funds wired to foreign country but no loss to institution

Recommended Action

- Your institution should have appropriate procedures for processing and cashing checks that include methods of identifying potentially suspicious items and criteria for placing holds on deposits



Recommended Action (cont.)

- Tellers should be trained to examine large-dollar checks more closely to identify suspicious checks, and to ask appropriate questions when persons deposit such checks.
- Your institution should be aware of the need to explain the status of deposits to its account holders clearly and accurately. For example, without such information, account holder may conclude that a check has cleared solely because the funds are available in the account holder’s account.

Recommended Action (cont.)

- Your institution should review your deposit agreements to insure that the agreements appropriately address returned items and mitigate the risks related to fraudulent checks.
- Regulators recommend that deposit agreements contain provisions which allow depository institution to charge back any item regardless of when the item is returned
- Therefore, even if depository institution made funds available, depository institution will still have contractual rights under the deposit agreement to charge back the item

Recommended Action (cont.)

- Your institution should consider methods of working cooperatively with account holders that become victims of check fraud.
- It may be appropriate in some circumstances to convert a resulting overdraft into a more formal loan that the account holder can repay over time, instead of demanding that the overdraft be repaid immediately.

What if You Think Your Depositor is a Co-conspirator?

- Example: Consumer deposits a check into his account and the check is later returned as fraudulent. The returned check causes an overdraft which the consumer doesn't have the money to pay. Consumer claims that he had a garage sale and sold something to this person.
  - This is when consumer pretends to be stupid instead of fraudulent
- Criminal Intent: Consumer has committed a crime if they knowingly participate in the scam and withdraw the fraudulent funds. But, there is no criminal intent if consumer is simply naïve and doesn't realize that it is a scam.

Debit Card Fraud (Consumer Account)

- Consumer's debit card allegedly had been used in retail stores in various States. Consumer had always had possession of debit card and had not been in those States.
  - Reg E applies
  - There was no loss of access device by the consumer, so the consumer liable for nothing during first 60 days
  - Your institution liable for everything
  - Your institution can't increase consumer's liability by contract

Commercial Account

- Uniform Commercial Code Article 4A generally permits institution to shift liability for online fraud activity to business customer if:
  - 1) There is a security procedure agreement between institution and business,
  - 2) Security procedure was commercially reasonable,
  - 3) Institution acted in good faith, and
  - 4) Institution complied with security procedure.

Important Contract Provisions

- Business agrees that institution's security procedures are commercially reasonable.
- Business acknowledges there may be other security procedures that are better or more state-of-the art than the institution's security procedures but the institution's security procedures are reasonable for the business' particular situation.
- Business agrees to be bound by any payment order that is accepted by the institution in compliance with the institution's security procedures, whether or not the payment order was actually authorized by the business.
- Require business to report online fraud activity within 24 hours, and failure to report within 24 hours causes business to bear entire fraud loss.

Wire or Other Online Fraud

- Example: Business is authorized to initiate wire transfers online. Among other things, one security procedure is a telephone call back if wire originated online or by email, or an email confirmation if wire originated by telephone. Bank receives email from authorized person on business account saying it is an emergency situation. The wire must go out today.
  - Bank will be liable if bank doesn't follow security procedure and criminal is pretending to be authorized party.

How Email Schemes Work

- Criminals access victim's e-mail account through social engineering or computer intrusion techniques.
- Criminals then use the victim's stolen information to e-mail fraudulent wire transfer instructions to the financial institution in a manner appearing to be from the victim.
- Criminals trick the victim's employee or financial institution into conducting wire transfers that appear legitimate but are, in fact, unauthorized. The fraudulent transaction instructions direct the wire transfers to the criminals' account.

How Email Schemes Work (cont.)

- *Scenario 1 – Criminal Impersonates a Financial Institution's Commercial Accountholder*: A criminal hacks into the e-mail account of Company A's employee to send fraudulent wire transfer instructions to Company A's financial institution. Based on this request, Company A's financial institution issues a wire transfer and sends funds to an account the criminal controls. *In this scenario, the criminal impersonating the financial institution's depositor prompted the financial institution to execute an unauthorized wire transfer*.

How Email Schemes Work (cont.)

- *Scenario 2 – Criminal Impersonates an Executive*: A criminal hacks into the e-mail account of Company B's executive to send wire transfer instructions to Company B's employee who is responsible for processing and issuing payments. The employee, believing the executive's e-mailed instructions are legitimate, orders Company B's financial institution to execute the wire transfer. *In this scenario, the criminal impersonating a company executive misled a company employee into authorizing a fraudulent wire transfer to a criminal-controlled account*.

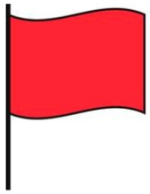
How Email Schemes Work (cont.)

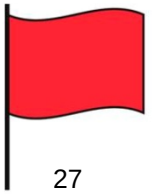
- *Scenario 3 – Criminal Impersonates a Supplier*: A criminal impersonates one of Company C's suppliers to e-mail and inform Company C that future invoice payments should be sent to a new account number and location. Based on this fraudulent e-mailed information, Company C updates its supplier's payment information on record and submits the new wire transfer instructions to its financial institution that direct payments to an account controlled by the criminal. *In this scenario, the criminal impersonating a supplier provided fraudulent payment information to mislead a company employee into directing wire transfers to a criminal-controlled account*.

Fraud Red Flags

- Seemingly legitimate e-mailed transaction instructions contain different language, timing, and amounts than previously verified and authentic transaction instructions.
- Transaction instructions originate from an e-mail account closely resembling a known account holder's e-mail account; however, the e-mail address has been slightly altered by adding, changing, or deleting one or more characters. For example:

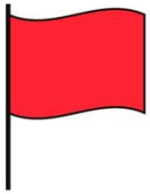
Legitimate e-mail address:	Fraudulent e-mail addresses:
john-doe @abc. com	john_doe @abc. com
	john-doe @bcd. com

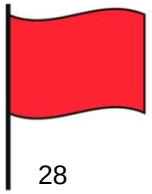




Fraud Red Flags (cont.)

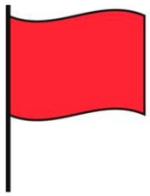
- E-mailed transaction instructions direct payment to a known beneficiary; however, the beneficiary's account information is different from what was previously used.
- E-mailed transaction instructions direct payment to a beneficiary with which the account holder has no payment history or documented business relationship, and the payment is in an amount similar to or in excess of payments sent to beneficiaries whom the account holder has historically paid.
- E-mailed transaction instructions include markings, assertions, or language designating the transaction request as "Urgent," "Secret," or "Confidential."
- E-mailed transaction instructions are delivered in a way that would give the financial institution limited time or opportunity to confirm the authenticity of the requested transaction.

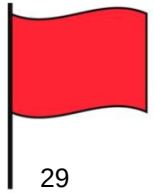




Fraud Red Flags (cont.)

- A company e-mails transaction requests for additional payments immediately following a successful payment to an account not previously used by the company to pay its suppliers/ vendors. Such behavior may be consistent with a criminal attempting to issue additional unauthorized payments upon learning that a fraudulent payment was successful.
- A wire transfer is received for credit into an account, however, the wire transfer names a beneficiary that is not the account holder of record. This may reflect instances where a victim unwittingly sends wire transfers to a new account number, provided by a criminal impersonating a known supplier/vendor, while thinking the new account belongs to the known supplier/vendor. This red flag may be seen by financial institutions *receiving* wire transfers sent by another financial institution as the result of e-mail-compromise fraud.





ACH Fraud

- Under NACHA rules, Originating Depository Financial Institution (ODFI) warrants that each payment is authorized, due and owing the originator, and is in compliance with NACHA rules
- Makes ODFI liable for unauthorized ACH under breach of warranty theory

ACH Fraud (cont.)

- Under NACHA rules, Receiving Depository Financial Institution (RDFI) can recover funds by means of return entries through NACHA system if return commercial ACH within 2 days or consumer ACH within 60 days.
- Even after the 2 day – 60 day period, RDFI can sue ODFI for breach of warranty until statute of limitations for breach of contract runs.

NACHA Operating Bulletin

- This warranty language is broad and does NOT limit itself to the period of time in which an RDFI can recover fund through the ACH Network by the means of return entries.
- An ODFI's potential liability under the NACHA Rules for breach of warranty is not limited to the return time frames, but is limited only by the statute of limitations for breach of contract claims under the applicable state law. For example, the ODFI's liability for breach of warranty exists for seven years in some states.

THANK YOU

If you have any questions regarding this presentation, you are welcome to contact the presenter:

M. Elizabeth Fast, Esq.
Spencer Fane LLP
Phone: (800) 526-6529 toll free
Email: efast@spencerfane.com