

Executive Fraud Forum on Payments Risk

Presented by:

PAUL A. CARRUBBA
Partner
Adams and Reese LLP

Paul Carrubba

- Paul is a partner in the law firm of Adams and Reese LLP. His primary focus is on Banking Law and legal issues dealing with payments system laws and regulations and bank operations issues. He has over 37 years of experience in the banking industry as a Bank Operations Manager, a consultant, an author, and an attorney. Mr. Carrubba is the author of five books including: *Revised UCC Article 3 and 4*, *A Banker's Guide to Checks* and *Principles of Banking*. He is the co-author, with Dan Fisher, of both *Remote Deposit Capture – Practical Considerations* and most recently, *Risk Management Series – Remote Deposit Capture*.

Presentation Content

THIS PRESENTATION IS DESIGNED TO PROVIDE ACCURATE AND AUTHORITATIVE INFORMATION REGARDING ITS SUBJECT MATTER. IT IS PRESENTED WITH THE UNDERSTANDING THAT THE PRESENTER IS NOT RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF LEGAL ADVICE OR OTHER EXPERT ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT.

Financial Institutions are the Targets of Law Suits – Does Your Institution have a Target on Its Back?



Obnibene v. Citibank

5

- Plaintiff was using the phone while another customer (the Crook) was pretending to be on the phone with customer service about a malfunctioning machine. Crook asked Plaintiff to enter his PIN in the machine to see if it worked, not once but twice. Court held that the transfer was NOT authorized and held Bank at fault for not warning Plaintiff and providing environment for fraud.
- Bank has burden of proof a PIN fraudulently obtained is not consent by the Customer even if the Customer is negligent

Marquess et al v. Penn. State Employees Credit Union; No. 09-4256
U.S. District Court, Eastern District of Pennsylvania

6

- Father, without No. 1 son's knowledge, opened account in name of No. 1 son with CU and forged No. 1 son's name to signature cards and authorization to transfer funds to father's and No. 2 son's account. Father died and No. 2 son transferred \$25,000 from No. 1 son's account through online banking. No. 1 son made a claim against bank.
- Court held that No. 1 son met the definition of a consumer under Reg. E and EFTA and held that the funds transfer was made with an access device that had not been accepted and Bank was liable. Court awarded treble damages.

CORPORATE ACCOUNT TAKEOVER CASES

UCC 4A

8

UCC ARTICLE 4A

- Applies to Funds Transfers
- Does Not Apply to Transfers Governed by EFTA (Reg. E)
- Authorized Transfers Enforceable
- Unauthorized Transfers Enforceable if:
 - Verified Pursuant to Security Procedure
 - Security Procedure is Commercially Reasonable
 - Bank Accepted it in Good Faith and in Compliance with Security Procedure

UCC 4A

9

UCC ARTICLE 4A

- Unauthorized Transfers Not Enforceable if:
 - ▣ Bank Agrees not to Enforce
 - ▣ No Security Procedure
 - ▣ Security Procedure is not Commercially Reasonable
 - ▣ Not Made by Authorized Person or Person Entrusted with Security Procedure
 - ▣ Not Made by Person who Obtained to Access to Transmitting Facility
 - ▣ Made by Person that Obtained Security Procedure from a Source not Controlled by the Customer

Security Procedures

10

Security Procedure

- Procedure to Verify Authenticity
- Procedure to Detect Error

Commercially Reasonable Security Procedure

- Question of Law Considering
 - ▣ Circumstances Known to Bank
 - ▣ Alternative Security Procedures Offered
 - ▣ Security Procedures in General Use

Cases

11

- Shames-Yeakel v. Citizens Financial Bank
- Experi-Metal v. Comerica Bank
- All American Siding V. Bank of America
- Patco Construction Company, Inc. v. Peoples United Bank
- Choice Escrow and Land Title, LLC v. BancorpSouth Bank
- Bank's Procedure Not Commercially Reasonable
- Bank did not Follow the Procedure

Shames-Yeakel v. Citizens Financial Bank

12

- Plaintiff Operated Accounting and Bookkeeping Company
- Linked HELOC to Business Account
- \$26,500 Unauthorized Transfer Made
- Ten Days Later, Plaintiff Contacts Bank
- Agreement Provides for Password and Company ID
- Expert Opined Security Procedures were Commercially Reasonable
- Plaintiff Claimed Bank did not Comply with 2005 FFIEC Guidance
- Court Held Procedures not Commercially Reasonable for Failure to Comply with Guidance

Experi-Metal v. Comerica Bank

13

- EMI Employee Responded to Phishing E-Mail
- Clicked on Site and Entered PIN, Password and Token Password
- Over 90 Transfers Initiated
- Bank Filed Motion for Summary Judgment
- Court Partially Granted Holding Security Procedures were Commercially Reasonable
- Did Bank Accept Transfer in Good Faith?
- Court Held Failed to Provide Evidence of Good Faith

All American Siding v. Bank of America

14

- Company ID, User ID, User Password
- Digital Certificate Installed on The Browser
- Dual Control on Wire Transfer (Rejected)
- Security Procedure Held Commercially Reasonable

Patco Construction Company, Inc. v. Peoples United Bank – DISTRICT COURT

15

- Unauthorized Transfers Totaling \$588,000 were made over Several Days
- Ocean Bank Blocked \$243,000
- Transfers Made from Unrecognized Device and IP Address
- Banks Security Procedures Included:
 - Password and ID
 - Challenge Questions
 - Risk Profiling
 - Device Cookies
 - Dollar Amount Rule
 - Subscription to eFraud Network
 - Customer Should Review Transactions Daily
 - Court Held:
 - Agreement Provided for Security Procedures
 - Course of Dealing
 - Both Parties Relied on FFIEC 2005 Guidance
 - Authentication was Multifactor and Layered Security
 - Security Procedure was Commercially Reasonable
 - Security Procedure does not have to be the Best
 - Patco Could have Mitigated Damages
 - Grants Summary Judgment Motion

Patco Construction v. Ocean Bank Court of Appeals

16

- Court of Appeals held security procedure was commercially **unreasonable**
 - Lowering the Dollar Threshold to \$1.00 increased the Risk of Fraud.
 - Ocean Bank did not Monitor the Transaction.
 - Ocean Bank did not Provide Notice to Customer.

Court of Appeals, cont

17

- Court Rationale:
 - ▣ System had risk scoring
 - ▣ If System detected Suspicious Transaction, additional layer of authentication was added – Challenge Question.
 - ▣ Since Bank did not monitor and report, Challenge Questions were asked each time and allowed Criminals to know the answers.
 - ▣ Ocean Bank's Service Provider warned against usage of Challenge Question as stand alone method.
 - ▣ The \$1.00 threshold ignored Article 4A – Customer circumstances.
 - ▣ Bank did not use Tokens.
 - ▣ Failure to implement additional procedures was especially unreasonable in light of the Bank's knowledge of ongoing fraud.
 - ▣ Payment order was uncharacteristic of Patco's ordinary transactions.
 - ▣ Risk scores were very high.

Choice Escrow and Land Title, LLC v. BancorpSouth Bank

18

- Plaintiff maintained Trust account with BancorpSouth.
- BancorpSouth received internet-based request to make wire transfer in the amount of \$440,000.
- Plaintiff asserts wire was fraudulently initiated by an unknown third party.
- Court concluded that this claim was covered by provisions of UCC.
- Court held that the security procedures were commercially reasonable.
 - Complied with FFIEC Guidance
 - Dual control is commercially reasonable
 - Customer refused Bank's security procedure and selected customer's security procedure
- Court held that Bank accepted the funds transfer request in Good Faith and in accordance with the Security Procedure.

AGREEMENTS

19

- ▣ Online/Internet Banking Agreements
- ▣ Wire Transfer Agreements
- ▣ ACH Origination Agreements
- ▣ Security Procedure
- ▣ Customer Agrees is Commercially Reasonable
- ▣ Customer Agrees to be Bound
- ▣ Customer will Safeguard Security Procedure
- ▣ Customer will Scan Personal Computer
- ▣ Customer will Give Notification of Unauthorized Transfer

Executive Fraud Forum on Payments Risk

PAUL A. CARRUBBA, Partner
Adams and Reese LLP
Phone: (601) 292-0788
E-Mail: paul.carrubba@arlaw.com