Recent Developments in Electronic Payments Law

April 24, 2017
Disclaimers

• The opinions expressed in this presentation are solely those of the presenter and do not necessarily reflect the opinions of NACHA or Dykema.

• This presentation is an educational tool that is general in nature and for purposes of illustration only. The materials in this presentation are not exhaustive, do not constitute legal advice and should not be considered a substitute for consulting with legal counsel. NACHA or Dykema does not have obligation to update the information contained in this presentation.
Agenda

• Hello from Hong Kong

• Jane:
  – ACH Arbitration (the “warm-up”)
  – Cybersecurity: Escalation and Regulation
    • Cyber attacks and everyone (seemingly)
    • Business email Compromise and FinCEN

• Erin:
  – Regulatory Developments
  – Policy Developments
  – The CFPB
Our Fulbright Scholar....working in the Salt Mines of Academia yet again (aka Hong Kong Harbor) sends her regards!!
The Warm Up
K&G Bank (RDFI) submitted an arbitration claim against B&B Bank (ODFI) citing improper reversal.

The RDFI claimed the following:

- Its customer received a PPD credit for remittance of an invoice in the amount of $5,200 with a settlement date of 8/12/16
- Its customer received a reversing PPD debit in the amount of $5,200 with a settlement date of 8/18/16
- Its customer was not notified of the reversing entry
- A representative of the ODFI told them that the reason for the reversal was due to a Third-Party Sender’s failure to receive funding from the Originator
Arbitration Continued

• Since the damages claimed in this case were less than $10,000, it was classified as an Arbitration Procedure A case and included one arbitrator.

• The arbitrator was provided with documentation from both the complainant (RDFI) and the respondent (ODFI), which included:
  – Summary of the events from each perspective
  – The respondent’s position that the reversal was done within the NACHA Rules:
    • The reason for the reversal was valid since the transaction in question was not intended for the Receiver
  – However, the complainant’s response included a voicemail from an employee of the respondent stating the reason for the reversal was a failure of the Originator to fund the TPS
After extensive review of the material, the arbitrator determined:

- B&B Bank had violated the Rules for reversing an entry for a reason other than those specified in the NACHA rules

Based on these facts, the arbitrator’s decision was:

- B&B Bank would reimburse K&G Bank the amount of the transaction ($5,200), the amount of the arbitration filing fee ($250), and pay the arbitrators’ stipend ($100)
Cyber
SWIFT Events

• Classic account takeover schemes on larger international scale:
  – $81 million theft from Bangladesh central bank
  – And a “meaningful” number of other attacks using a similar approach
    – including attacks on Polish banks

• Attacks were sophisticated but used known tactics such as phishing to steal credentials and gain system access to banks

• After gaining access the attackers initiated fraudulent transfers and committed alleged thefts

• The thefts were the result of sub-optimal infrastructure management (e.g., lack of firewalls, inexpensive routers, etc.)
And Now It Gets Interesting......

“North Korea’s Rising Ambition Seen in Bid to Breach Global Banks”

New York Times March 25, 2017

“Bankers beware: North Korea is on a hacking spree”

Locked in a punishing sanctions regime, North Korea is throwing caution to the wind and has mounted a series of cyber attacks by taking advantage of outdated financial technology, mainly through the SWIFT network. Such cyber-attacks are likely to continue if international financial systems are not shored up in the near future.

globalriskinsights.com
Regulatory Complexity

• In response to high profile cyber attacks, there has been an increased focus from regulators which illustrate different approaches to the cyber issue
  – New or revised regulation
  – Raised awareness; and
  – Enforcement
Regulatory Complexity

- There is already an expansive and complex web of regulator-issued cybersecurity rules and guidance that FIs must adhere to voluntarily or by requirement:
  - Interagency Security Guidelines issued pursuant to Gramm Leach Bliley – requires FIs to implement an info sec program covering administrative, technical and physical safeguards to protect consumer’s personal information.
  - Many agencies have expressed support for – and many FIs utilize the National Institute of Standards and Technology (“NIST) Framework for Improving Critical Infrastructure Cybersecurity as a resource to assist companies in developing and implementing a cybersecurity policy – not specific to FIs. Voluntary and customizable.
  - The FFIEC Information Security Booklet – updated in September 2016 contains Guidance that applies to all FIs. FIs may use the Cybersecurity Assessment Tool as a “repeatable and measurable process” to measure an FI’s cybersecurity preparedness over time.
Federal: Advanced Notice of Proposed Rulemaking on Enhanced Cyber Risk Management Standards

- Published in Oct 2016 by the FRB, the OCC and the FDIC (the “Agencies”). Comment closed Jan 2017
- Goal: to strengthen the operational resilience of large and interconnected financial entities and by doing so reduce the likely impact of a cyber event on the financial system as a whole
  - Also applies to third party service providers w/respect to services provided to FIs and their affiliates that are covered entities
    - either directly or indirectly
- Could require significant new efforts to implement compliant processes and manage them over time
- Makes many currently voluntary programs/processes mandatory
- Does not articulate gaps in current patchwork of cyber regulations and guidance
- Could have trickle down effect
State: New York Department of Financial Services

- Proposed “First in Nation” rules in September of 2016 to require FIs, insurers and others to establish and maintain cybersecurity programs to protect consumers and the system “to the fullest extent possible” against cyber attacks.
- Received (many! very critical!) comments and revised and resubmitted in December 2016 – revised proposal more ‘risk-based’
- Requires a written cyber security policy based on a risk assessment. It mirrors much of what already exists, but there are some unique features, including:
  - Requirement that a covered entities designate a CISO
  - The use of multi-factor authentication before permitting someone outside the network from accessing internal systems
  - Requiring the destruction of records after their business purpose has expired
- Greater question: what if other binding cyber standards deviate from or conflict with NY? Is a state by state approach best?
Purpose: to assist FIs in understanding their BSA obligations regarding cyber-events and cyber-enabled crime

To determine whether a cyber-event should be reported, an FI should consider all available information, incl. the nature, information and systems targeted during the event, and also in aggregate the funds and assets involved in or put at risk by the event.

Examples of cyber-events that trigger mandatory reporting include:
- A malware intrusion that is suspected to put at risk $500,000
- A hack that exposes customer information
- A DDOS attack that is used to cover up an unauthorized wire transfer

FinCEN encourages sharing within FIs and also information sharing b/w FIs as allowed by the Safe Harbor provided by the Patriot Act
Business eMail Compromise
Vendor/CEO Impersonation

• Business email compromise: depending on facts, can be less sophisticated and potentially more effective than corporate account takeover because victim actually interacts with FI and approves payment to be sent
  – Can be internet based or can be “old school”
• FBI estimated that between Oct 2013 and Aug 2015 thieves stole $750 million from over 7000 victims
• The majority of transfers going to FIs in China and Hong Kong
• ACH Operations Bulletin #1-2017: Social Engineering Fraud Against Public-Sector and Other Entities
FIN-2016-A003

• Purpose: to help FIs guard against a growing number of e-mail fraud schemes where thieves misappropriate funds by deceiving FIs and their customers into conducting wire transfers

• The Advisory refers to different scenarios, but generally two types of compromises:
  – Where the thief induces a customer to initiate a funds transfer (the customer authorizes the wire)
  – Where the thief itself directly interacts with the FI - impersonating the customer to instruct the bank to send a wire transfer

• Advisor lists many red flag to use in the review and verification of customers’ transaction instructions

• Potential problems:
  – Seemed to suggest that both types of scenarios result in unauthorized transactions despite customer having authorized the payment
  – Many of the red flags not realistic in an automated environment
  – Unintended consequences of Advisory
Erin
Regulatory Developments
• **OCC: Comptroller Curry announces OCC “Limited Purpose” Charter framework at Georgetown Law Center (12/2/16)**
  – OCC simultaneously released proposed framework for the OCC “Fintech” Charter
    • Comment in framework that even if Community Reinvestment Act does not apply, OCC still going to examine financial inclusion initiatives
  – Comment period on proposed framework ended 1/15/17

  – Follows other OCC activities earlier in 2016
    • **May 2016 OCC Whitepaper**: “Supporting Responsible Innovation in the Federal Banking System: An OCC Perspective (set forth OCC’s principles for responsible financial services innovation)
    • **June 23, 2016**: OCC Forum on Responsible Fintech Innovation
• **OCC: Comptroller’s Licensing Manual Draft Supplement “Evaluating Charter Applications From Financial Technology Companies”**
  
  – **March 2017**: released along with an OCC “Summary of Comments and Explanatory Statement”; over 100 comments submitted to OCC
  
  – Many non-bank lenders, payment services firms and their trade associations strongly support the proposal and want OCC to provide more flexibility
  
  – Many community and regional banks, state regulators and attorneys general expressed concern that special purpose charter would hold chartered firms to less stringent consumer protection requirements and safety and soundness standards, and encourage regulatory arbitrage
  
  – **OCC’s Response:**
    
    • OCC will not allow inappropriate commingling of banking and commerce
    • OCC will not allow products with predatory features or allow UDAP violations
    • No “light-touch” supervision and chartered entities will be held to same standards
• Conference of State Bank Supervisors (CSBS) Response
  – On 12/2/16, CSBS issued a press release containing its response to the OCC’s Fintech Charter framework
    • Based upon CSBS comments, CSBS disagrees with the need for an OCC Fintech Charter (among other issues regarding the proposed OCC Fintech Charter)
    • From CSBS Press Release:
      – State regulators concerned that OCC’s subjective criteria for awarding “limited purpose” charters, and its intent to not include the normal regulatory safeguards placed on national banks (such as deposit insurance) would result in the OCC choosing winners and losers within the Fintech industry and broader banking industry
      – National Bank Act does not give the OCC authority to issue full-service bank charters to institutions that do not engage in deposit taking and there is no historical precedent for this
      – CSBS believes this will ultimately put consumers at risk because OCC formerly preempted state anti-predatory lending laws for national banks and their subsidiaries “thereby permitting unsafe and abusive lending practices to flourish in the lead up to the financial crisis”
      – BUT question remains regarding what about fintech startups that will not be able to meet any OCC minimum capital requirements. What do they do? Partner up?
• State Regulation and Innovation
  – Nationwide Multistate Licensing System & Registry (NMLS) (owned by CSBS)
    • Web-based system that allows state-licensed non-depository companies, branches, and individuals in the mortgage, consumer lending, money services businesses, and debt collection industries to apply for, amend, update, or renew a license online for all participating state agencies using a single set of uniform applications.
    • Mortgage loan originators employed by insured depository institutions are also registered through NMLS.
    • April 1, 2017: the NMLS Money Services Businesses (MSB) Call Report was released in NMLS. Multi-year effort by state regulators to develop a tool to standardize and streamline routine reporting requirements for state licensed Money Services Businesses. Licensees submit the report directly in NMLS through a single interface for all states on a quarterly and annual basis. 18 states participating for Q1 2017 reports.
    • Additional changes/features for “NMLS 2.0” being developed
  – Texas Department of Banking: Potential “startup” form of money transmission license
    • “Startup” is a company that has started business operations within last 5 years and has never engaged in money transmission
    • Creates a limited purpose Money Transmission License In Texas for startups. No more than 3 years max before has to meet full MTL (or upon sale/merger or exceeding max operational thresholds to be established by TxDOB Rule)
    • Startup must have a “sponsor” that is either a licensed entity under Texas MTL law or otherwise exempt
    • On hold for now and not proposed in 2017 legislative session
• **Uniform Law Commission: Currently Drafting “Regulation of Virtual Currency Businesses Act”**
  
  – Some states, including New York and California, are currently examining ways to regulate virtual currencies, and others are soon to follow.
  
  – In the absence of an overarching federal payments regulatory framework, these state laws need to be harmonized to the extent possible.
  
  – Drafting committee will consider the need for and feasibility of drafting state legislation on the regulation of virtual currencies, and will examine issues such as licensing requirements; reciprocity; consumer protection; cybersecurity; anti-money laundering; and supervision of licensees.
  
  – **Active comment process on the iterative drafts so far from industry and others**
  
  – Very interesting components, including a proposed “de minimus” exemption (currently $50K or less), “on ramp” license phase (over $50K up to higher dollar amount yet to be determined), and full licensing above the upper cap for on-ramp
  
  – Also, provides for potential for different levels of reciprocity from common licensing application up to full reciprocal licensing (State A can accept and approve license based on company being licensed in State B)
  
  – New draft of the model act is coming very soon (next few weeks)
Policy Developments
• **Financial Innovation Now ("FIN")**
  
  - Amazon, Google, Apple, Intuit, etc.; **Nov. 30, 2016**: sent letter to Trump-Pence Transition Team with Fintech Regulatory Agenda “Wish List”
    - Appoint a new U.S. Undersecretary of the Treasury for Fintech Strategy
    - Promote open, interoperable standards for card payment security and get rid of closed and proprietary networks that lock out innovation
    - Streamline money transmission licensing by working on streamlined federal money transmission licensing system (protects consumers and fosters innovation)
    - Ensure consumer access to financial accounts and data and prevent financial institutions from blocking consumer-granted access to such information
    - Streamline small business access to capital via the internet and work at the federal level to streamline antiquated state lending laws
    - Real-time payments network for all Americans by 2020
    - Leverage mobile technology to increase financial inclusion
• **American Banker’s Association 2017 Legislative Agenda for Fintech**
  
  – Facilitate partnerships of banks and technology firms

  – Ensure customers are protected through consistent and effective oversight of all (i.e. non-bank) providers

  – Encourage innovations by providing a regulatory “greenhouse” (a/k/a “regulatory sandbox”) for testing new products before they roll-out (something more than CFPB’s Project Catalyst but more robust?)

  • **TIP:** Whenever anyone makes reference to the “sandbox” or “regulatory sandbox” concept for Fintech, they are typically referring to the U.K.’s Financial Conduct Authority’s development and testing “regulatory sandbox”
• American Banker’s Association 2017 Legislative Agenda for Fintech
  – UK Financial Conduct Authority (Cont’d)
    – FCA developed Project Innovate to foster competition and growth in financial services by supporting both small and large businesses that are developing new products and services that could genuinely benefit consumers. In its first year (2014 – 2015) Project Innovate helped over 175 innovative businesses.

    – In 2015, FCA expanded Project Innovate to introduce a “regulatory sandbox” that is a “safe space” in which businesses can test innovative products, services, business models and delivery mechanisms “without immediately incurring all the normal regulatory consequences of pilot activities.”

    – Fintech developers like the concept of the “regulatory sandbox” because it mirrors the product development cycle and allows them to test the viability, functionality and scalability of their products and services prior to full public launch.
EU “Payment Services Directive 2” (PSD2)

- Effective Jan. 12, 2016; lots of additional deadlines in Jan. 2018
- Lays down the foundation for open banking APIs in EU
- While that is focused on technology standards that allow non-banks to obtain information necessary to conduct transactions, what about other data?
- **March 2017**: European Banking Authority essentially outlawed “screen scraping”
- The EBA suggests that banks can deny this type of “direct access” through their front door, if they are providing another “indirect access” possibility via a new to be developed API at their back door.
- Addresses security and access concerns for banks, while still allowing access to customer data (just controlled access).
- **U.S. Policy Implications**: Are “open data” (CFPB looking at this) and “open API’s” the same or qualitatively different?
The CFPB
• **Prepaid Card Rule**
  - CFPB Final Prepaid Card Rule and application of Reg E to certain types of mobile wallets (FYI may be undone by Congress under Congressional Review Act)

  • The new rule — despite objections from Google, PayPal and others - covers “digital wallets capable of person-to-person transfers and storing funds.” Square Inc.’s Square Cash and Dwolla’s payment tool will also arguably fall under the new rules.

  • Wallets like Apple Pay — which simply store payment credentials issued by banks — will not fall under the new rule (logic being that the underlying payment account is subject to Reg E
• **CFPB vs. Intercept Corp.**
  
  – **June 2016**: CFPB files complaint against third party payment processor Intercept Corp. alleging UDAAP violations, including processing transactions for clients, including consumer lenders, when Intercept knew/should have known transactions were fraudulent and illegal.

  – **Specific allegations:**
    • Failed to heed warnings from banks and consumers that processing customer activities were illegal and debits not authorized by consumers
    • Failed to adequately monitor and respond to high rates of transaction refusal/rejection
    • Ignored law enforcement activity related to processing customers and continued processing despite these law enforcement red flags
    • Failed to investigate red flags in customer application/due diligence process (focusing only on risk assessment that only determined processing customer’s ability to pay)

  – **March 17, 2017**: U.S. District Court for Easter District of ND dismissed “without prejudice” CFPB’s complaint against Intercept and 2 Intercept executives for failure to state a claim
    • CFPB did not allege facts demonstrating consumers were injured or likely to be injured by Intercept’s actions (vs. processing customer’s actions)
    • No facts allowing defendants or court to determine whether any potential injury was outweighed by countervailing benefits to consumers (UDAAP elements)
    • NOTE: “Dismissed without prejudice” means CFPB can cure deficiencies in pleadings and re-file
CFPB Customer Data Inquiry

CFPB Developments (cont’d)


- Lots of high-profile FIs have taken prominent action against “screen scraping” (practice where non-bank third party gets bank customer to turn over log-on credentials for bank account and third party grabs the data)

- Banks believe that it is inherently insecure for an unvetted third party to obtain highly sensitive logon credentials, so FIs like Wells Fargo create secure APIs to allow banks to push data

- Screen scraping is old, outmoded, won’t work with 2 factor authentication, and what about FI’s security obligations under GLBA

- CFPB wants to find out how much control consumers have over their records and how easy and secure it is to share records (privacy vs. security argument)
• CFPB Customer Data Inquiry (cont’d)

  – 3 “Themes” of 70 Comments Submitted in to the CFPB Inquiry

• Theme 1: Does Dodd-Frank Mandate Access To Third Parties?

• FinTechs (like Affirm, Betterment, Digit, Envestnet Yodlee, Kabbage and Personal Capital) say that Section 1033 of Dodd Frank “codified the consumer’s right to access their personal financial data through technology-powered third party platforms

• Banks/FIs: WRONG! Consumers have rights, but third parties do not have a codified right. Requiring financial institutions to allow a third-party to access a consumer’s account online goes beyond the current requirements, conflicts with the Gramm-Leach-Bliley Act, and introduces substantial consumer data security risks.
• Consumer Protection (cont’d)

– 3 “Themes” of 70 Comments Submitted in to the CFPB Inquiry (cont’d)

• Theme 2: Financial Institutions Profit Off Of Complexity And Sub-Optimal Decisions, Third Parties Using Aggregated Data Offer Transparency

• Academic Comments: The sellers of financial products have an incentive to withhold from providers their customers’ financial information because they make money when complexity causes customers to make sub-optimal decisions.

• FinTechs: We can inform consumers whether their offer is market, above market, or below market, and whether there are different credit products that are a better fit for their financial profile. This transparency and ease of comparison in turn can spur more innovation and competition in the market of consumer financial products. (Credit Karma)
• Consumer Protection (cont’d)

   – 3 “Themes” of 70 Comments Submitted in to the CFPB Inquiry (cont’d)

   • Theme 3: Data Aggregators Are Financial Institutions Subject to Gramm-Leach-Bliley (GLBA)/Reduce The “Disparity In Data Security Expectations And Practices Between Banks And Data Aggregators”

   • CFPB should clarify that data aggregators are "financial institutions" subject to the requirements of GLBA
   • CFPB should take steps to ensure data aggregators are subject to the same standards as depository institutions for safeguarding financial data and notifying customers about security breaches
   • CFPB should clarify that data aggregators are “service providers” under the Electronic Funds Transfer Act (EFTA) and are liable for unauthorized electronic fund transfers that exceed the consumer’s liability under EFTA (ABA, The Clearing House, Capital One)
   • Some FinTech’s voluntarily comply with GLBA (e.g. Plaid)
• CFPB and “Consumer Control” of Data

  – Would open APIs have to be secure AND subject to the choices of the consumers as to what financial data they want to disclose?

  – FI “ownership” rights in data (or gatekeeper of data?)

  – Security concerns

  – U.S. version of PSD2 to compel financial institutions to provide account information to third parties via application programming interfaces (APIs)?
Erin F. Fonté, CIPP
Member
Payments, Fintech and Digital Commerce
Financial Institutions Regulatory & Compliance
Dykema
111 Congress Avenue, Suite 1800
Austin, Texas 78701
Direct: 512-703-6318
efonte@dykema.com
@PaymentsLawyer
Linkedin Link me in: Erin Fonte