Payments Fraud, Risk Management, & EMV

Mid-South AFP

Oct. 23, 2014

Matt Davies, AAP, CTP, CPP
Federal Reserve Bank of Dallas

FRB Dallas Payments Fraud Survey

- FRB Dallas, collaboration w/ other FRBs, and ICBA of America
- Addressed payments-related fraud experiences of banks and businesses
- Goal: Better understand new or continuing challenges with payments fraud, and methods used to reduce fraud risk
- Five TX AFP/TMA chapters also distributed to members
- Survey results:

  Dallas District:
  http://www.dallasfed.org/assets/documents/banking/firm/fi/fraud_survey.pdf

  National: http://www.minneapolisfed.org/about/whatwedo/payments/2012-payments-fraud-survey-consolidated-results.pdf

FRB Dallas Payments Fraud Survey

- Payment-related fraud remains a significant concern for financial institutions (FIs) & corporates
- For FIs, signature debit card is the payment instrument most vulnerable to attempted fraud & FI losses
- For non-FIs, check continues to be the payment instrument most vulnerable to attempted fraud & losses

FRB Dallas Payments Fraud Survey

- Corporate account takeover can result in significant losses, but was not identified as a commonly-occurring fraud scheme that affected a high percentage of respondents to this survey*
- Most FIs & others report total fraud losses that represent less than 0.3% of their annual revenues
- Strategies to detect & prevent fraud effectively require the use of multiple mitigation methods & tools – i.e., a “layered” strategy

FRB Dallas Payments Fraud Survey

- Two-thirds of respondents that reduced their fraud losses cited as factors:
  - Enhanced fraud monitoring systems
  - Employee education & training
- Offering risk mitigation services to customers is a growing area of opportunity for FIs
- Cost is the main barrier that prevents FIs & others from investing more in mitigating payments fraud
- FIs & others are focused now on the need for alternatives to magnetic stripe authentication technology to secure card payments [=EMV]

AFP Fraud Survey

- 2013 AFP Payments Fraud and Control Survey
  - Organizations generally do not change out affected bank accounts after experiencing fraud. Instead:
    - Rely on established controls to identify additional incidences (38%), or
    - Make adjustments such as changing the check series or adding new controls (24%)
  - Best practice: Daily reconciliation
  - Best practice: Segregating accounts: 74% of organizations maintain separate accounts for different payment methods and types.

Check/Check 21 Fraud Prevention

- Positive Pay/Reverse Positive Pay/Positive Pay with Payee Verification
  - 2010 check fraud case: Cincinnati Insurance Co. v. Wachovia Bank
- Make large dollar payments electronically.
- Avoid using laser checks.
- Use a controlled stock of high security checks, with safety features such as a true watermark, thermochromatic (heat sensitive) ink and reactivity to various chemicals.

Mobile RDC

- Risk: “Double Dipping” (or Triple, etc.)
- Risk mitigation:
  - FIs that offer mobile RDC should have protections in place to block duplicate deposits
  - Do not have to offer mobile RDC to all customers; “qualify”
  - Typically limit the dollar amount that can be deposited (daily, monthly)
  - Restrictive endorsement
- Hacks waged against mobile will likely increase.
  - As more FIs launch mobile RDC, those threats will grow.

Corporate Account Takeover (CATO)

- Account takeovers have grown more common, as fraudsters go after smaller businesses and smaller banks, where security is often weaker.
- Many small business owners are no more savvy about risks than the average consumer

Corporate Account Takeover

- Individual Americans are protected by Reg E & are liable for a maximum $50 if a cyber-thief strikes.
- Companies have no such guarantees.
- In the US, corporate customer liability is governed by the Uniform Commercial Code (UCC).
- Companies are responsible for stolen funds if:
  - they have agreed to a security procedure with the bank,
  - the bank followed it, and
  - the procedure was ‘commercially reasonable.’

FFIEC Guidance

- **FFIEC Supplemental Guidance on Internet Authentication**
  - Released June 2011
  - Supplement to *Authentication in an Internet Banking Environment* guidance issued October 2005
  - Lays out broad steps banks should take to guard against malware attacks.
  - Reaffirms the need for banks to conduct risk assessments at least once a year
  - Establishes minimum requirements for educating customers about online fraud.

FFIEC Guidance

- Prescribes layered security for business accounts
  - Includes the ability to detect and respond to suspicious activity when logging in and initiating transactions.
  - Stop relying on tokens, passwords and cookies
  - Instead, use “layered security,” including software that flags unusual behavior such as multiple transfers within minutes to new recipients
- Directs FIs to add security for business accounts, including enhanced controls over admin functions, where privileged users’ passwords, if stolen, can give hackers direct access to a company’s bank accounts.
- Does not endorse any specific technology for doing so
- FIs should make clear to business customers that they are not protected by Reg E.

Corporate Account Takeover

- Experi-Metal - Small parts supplier for US auto industry, based in Michigan
- Signed up for online banking in 2000
- “Regularly received e-mails from the bank with instructions”
- Jan. 22, 2009 – Controller received a fraudulent e-mail appearing to come from Comerica directing him to fill out a ‘Comerica Business Connect customer form,’ including his user name, password and pin from a token (7:35 a.m.)

Comerica vs. Experi-Metal

- By 2:02pm, 93 payment orders had been issued in Controller's name, sending $1.9m to accounts in Russia, Estonia and other places where Experi-Metal had never done business
  - According to court records, had sent such wire transfers only twice in the previous 2 years
- Four hours into events, JPMC, party to 6 transfers destined for customer accounts at Alfa-Bank, Moscow, called with suspicions. Still, a further hour and ½ passed before Comerica stopped the transfers
- Fraudulent wire transfers totaled more than $1.9m; Company lost $560,000

Comerica vs. Experi-Metal

- Experi-Metal sued Comerica; case tried in Detroit in 2011.
- Verdict: Experi-Metal
  - While the regulatory guidance then in effect did not require better monitoring, Comerica was not acting in good faith if it had a “pure heart and empty head.”
  - Cited numerous oddities about the transactions and the slow reaction when JPMC called
  - Concluded that “a bank dealing fairly with its customer, under these circumstances, would have detected and/or stopped the fraudulent wire activity earlier.”
  - Ordered Comerica to reimburse Experi-Metal $560,000; settled in August 2011 for an undisclosed amount.

PATCO v. People's United

- PATCO Construction (Maine) vs. former Ocean Bank (now Peoples United)
  - Court delivered a different legal outcome.
  - Case spurred by the fraudulent ACH transfer of $545,000 in May 2009
  - Magistrate sided with the bank
  - PATCO appealed the ruling

PATCO v. People's United

- 7/3/2012: Appeal Verdict: PATCO
- Further recommended that the two parties pursue an out-of-court settlement of the case.
- Ruling describes the bank's security procedures as "commercially unreasonable"; bank should have detected and stopped the fraudulent transactions

PATCO v. People's United

- Decision demonstrates that effective data security is not just about the **technology**; it is equally about **people**.
- The bank's system allowed for:
  - Used by the bank: UID & password, customer device recognition by IP address & cookie, transaction risk profiling, challenge-response based upon shared secrets, dollar amt. threshold for invoking challenge-response, access to intelligence from the eFraud Network including IP addresses of known hostile systems
  - Not used by the bank: one-time-password tokens, **out-of-band authentication**, user-selected image for recognizing the bank, risk scoring reports

PATCO v. People's United

- Court's decision: The heart of the problem was not with the technology, but with the way the bank used (or did not use) it
  - Bank triggered challenge questions for any transaction over $1.
    - This increased the frequency with which a user was required to enter answers to challenge questions;
    - increased the chance that authentication info could be stolen by hackers (e.g. through a keylogger or other malware).
  - When the system triggered warnings that fraud was likely occurring, bank personnel did not monitor transactions, or provide notice to customers before allowing transactions to be completed.
  - Bank personnel did not monitor risk-scoring reports.
  - Bank did not conduct regular reviews of transactions that generated high risk scores.

PATCO v. People's United

- Bank employees should have been aware of the increased risk of compromised security; at the time, keylogging malware was a "hot topic" in the financial industry (and continues to be).
- Bank personnel should have understood that triggering the same challenge questions for all transactions (high-risk and ordinary) was not effective as a stand-alone backstop to password/ID entry.

PATCO v. People's United

- Bank's decision to set dollar amount rule at $1 for all customers ignored legal requirement that security procedures take into account **"the circumstances of the customer"** known to the bank.
- Bank was using OSFA approach
- Other banks' clients using the same security product employed manual reviews or some other security measure to protect against the type of fraud that occurred in this case.

SOURCE: "Appellate Court Decision Demonstrates Security Is Not Just about Technology – It's about People," Foley & Lardner LLP, 8/16/2012

Choice Escrow & BancorpSouth

- 2010: Choice Escrow & Land Title; hackers wired $440,000 to a bank in Cyprus.
- Choice sued BancorpSouth Bank for failing to provide "commercially reasonable security," demanding damages and recovery of losses related to the attack.
- 2012: The bank filed a counter-suit; US district court in Missouri dismissed the counter-claim, though judge said it was a "very close call."

SOURCE: "US court dismisses bank's counter-suit against hacked customer," *Finextra,* Aug. 29, 2012

Choice Escrow & BancorpSouth

- March 2013: U.S. District Court for the Western District of Missouri rejected Choice's suit against BSB.
- Decision based on the fact that Choice declined to use security measures BSB had encouraged it to use.
- When Choice adopted online banking in 2009, BSB usually required customers to use dual control for wires.
- Choice declined dual control as an inconvenience, as the employee who handled wires was often in the office by herself.
- Choice appealed; verdict upheld in favor of Bank (+ legal fees!)

Dual Control

- Alternatives for customers that are too small to have dual custody (e.g., a company only has two employees)?
  - E.g., Wells Fargo this year introduced a feature called secure validation.
  - When a customer submits a payment, the bank can text or call the user's mobile device and provide a number that the customer then has to enter in a field on the site.

Future Trends

- Trends in CATO:
  - Malware Goes Mobile
  - Same-Day ACH?

Prevention of CATO

- A wealth of info online about CATO.
- Basic principles:
  - Daily account reconciliation
  - Employee education
  - Security
  - Multifactor authentication
  - Dedicated PC(s) for performing online banking functions
  - Limit use of social networks, personal e-mail, and general Internet usage

Prevention of CATO

- Preparedness: A company's risk profile/risk assessment should include information about CATO.
  - How will you attempt to prevent it (operational)?
  - How will you mitigate the risks associated with it (financial/reputational)?
  - Each organization's plan may vary.

Prevention

- NACHA, “Sound Business Practices for Companies to Mitigate Corporate Account Takeover”
  https://www.nacha.org/userfiles/File/Sound%20Business%20PracticesBusinessesFinal042811.pdf
  - Use of firewalls, antivirus, anti-spyware, anti-malware, etc., is often touted for preventing corp. acct. takeover. Are you using these?
  - More importantly, are you using products that form a “suite”? “Security programs from multiple companies sometimes do not work well together, often working against each other.” [NACHA]
  - Minimize the number of employee user accounts with admin rights; many malware programs can infect a PC only if the user has admin rights.
  - Restrict use of flash drives to those provided by your IT dept.

“In Case of Emergency. . .”

- Employee education is crucial; employees should know whom to notify and how regarding any suspicious activity.
- Corporates: Work with FI to ensure online access to user accounts is disabled; all online banking users will need to change online banking passwords, or open new accounts, if necessary.
- FIs: Review all recent transactions and authorizations on the account; if any are suspicious, cancel or reverse them ASAP (if possible).
- FIs: Ensure that hackers have not created any new users or payees, requested a change of information such as address or phone number, changed access levels of any user, altered ACH batch or wire transfer templates, or ordered new cards, checks or other documents.

"In Case of Emergency. . ."

- File a police report.
  - May help you in working with FIs, insurance companies or other entities that may need to be involved in subsequent investigations.
  - Keep detailed records of what has happened and steps you have taken to resolve the situation.
- You may need to take additional action if your organization accepts credit cards.

DDoS Attacks

- Distributed Denial of Service (DDoS)
- May be used to distract/confuse security staff at FIs to initiate fraudulent wire transfers
- NOT like the high-volume DDoS attacks which, last year, have brought down many U.S. FIs' sites
  - Politically motivated; no thefts associated

DDoS Attacks

- 2/2013: Brian Krebs, security blogger, reported a 12/24/2012 event at Bank of the West; DDoS used as a distraction
- $900,000 loss
- Once the DDoS is underway, hackers take over the payment switch (e.g., wire application), using a privileged user account which can access it.
- Hackers can then control the payment switch and move money from accounts, until they are discovered.
- If you are /your FI is under a DDoS, pay attention to wire system

Tax Return Fraud

- ID thieves file fake federal returns using taxpayers' SSNs; taxpayer files subsequently and the return is rejected, as someone already filed a return and received a refund using that identity.
- 641,052 taxpayers affected by ID theft in 2011, more than double the number affected in 2010
- IRS detected 940,000 fake returns for 2010, in which ID thieves tried to obtain $6.5 billion in refunds

Tax Return Fraud

- Prevention:
  - IRS now uses a code to identify taxpayers who have died, so their numbers cannot be used by thieves
  - IRS has issued more than 250,000 identity protection numbers to ID theft victims to use to prove they are the legitimate taxpayers when they file returns.
  - IRS will be implementing measures to resolve cases faster.
  - Taxpayers should guard SSN, and file tax returns as early as possible

SOURCE: Eileen Ambrose, "Protect Your Tax Return from Identity Thieves," *The St. Louis Post-Dispatch,* Sunday, May 27, 2012, p. D2

Fraud Prevention for Merchants

- Check acceptance?
  - Some merchants (e.g., Wendy's) do not accept checks
- Manual entry of card transactions?
  - One large convenience store chain has disabled the ability for its cashiers to key-enter transactions.
  - This led to a significant decrease in fraud
- Storage/use of customer data?

EMV

- “EMV” = Europay, MasterCard, and Visa
- 1994: Founded the global standard for credit and debit payments based on chip card technology.
- Today, EMV standards are set by EMVCo, a joint venture of Visa, MC, AmEx, JCB, Discover and UnionPay.

EMV

- "Chip cards," "chip and PIN cards," and "smart cards" are used interchangeably.
  - Plastic cards that contain a microchip that sends a dynamic protected value unique to each transaction
- Though "chip and PIN" is often used with EMV, the standards allow for cardholder verification via signature (PIN is most common in other countries).

EMV

- EMV standards have been adopted in many other countries, but the U.S. has lagged behind.
  - Reluctance due to the cost of changing payment terminals to accept chip payments.
  - Some U.S. card issuers have begun issuing cards containing EMV chips (e.g., to frequent international travelers so that they don't have payments problems abroad), but many have yet to move in that direction.
  - The cost of terminal and card migration may be as high as $12bn (Javelin).

Dynamic Authentication

- EMV relies on dynamic authentication: use of changing variables unique to each individual card transaction
- When mag-stripe cards are swiped at POS terminal, data, such as primary account number (PAN) and expiration date, are transmitted to the card issuer.
- The data—known as static data—remains the same for each transaction.

EMV

Two Ways of Accepting Chip Card Payments

- **Contact ("dipping" the card):** Cardholder inserts card into POS device. Card remains in device until completion of the transaction. If a customer removes the card before the charge is approved, the transaction will fail and the customer will be required to provide the card again.
- **Contactless ("tap-and-go"):** Cardholder waves the card by the chip card-enabled POS device to provide payment information. Once the transaction has been authorized, customer might then be prompted to enter PIN or sign a receipt. [See also, Apple Pay!]

Card Associations & EMV

- Visa roadmap to EMV (August 2011)
  - Expand TIP: Visa will expand its Technology Innovation Program (TIP) to merchants in the U.S.
    - Merchant must still *be* PCI compliant, but…
    - TIP ends the mandate for merchants to *validate* compliance with the PCI Data Security Standard (PCI DSS) for any year in which 75% of the merchant's Visa transactions stem from chip-based terminals.
    - To accommodate the Visa mandate, merchants must use terminals that support both contact and contactless chip technology.

Card Associations & EMV

- Liability Shift: Visa will institute a U.S. liability shift for counterfeit card-present POS transactions, eff. Oct. 1, 2015.
  - MasterCard, AmEx and Discover have adopted the same date
  - Currently, POS counterfeit fraud is largely absorbed by card issuers
  - After liability shift, if a contact chip card is presented to a merchant that has not adopted, at minimum, contact chip terminals, liability for counterfeit fraud may shift to the merchant's acquirer.
  - The acquirer will likely shift that liability down to the merchant.

Liability Shift

- Fuel-selling merchants have until Oct. 1, 2017, before liability shift takes effect for transactions at automated fuel dispensers, due to the added expense of updating.
- NACS (2012): Average card fraud costs at fuel pumps at each store, about $700 a year, but PCI security standards costs were rising to about $2,000 a year.
- Average cost of EMV conversion per pump: $6-10k

David Heun, "Gas Stations Face EMV Sticker Shock," *PaymentsSource*, Oct. 7, 2014

Card Associations & EMV

- Liability shift to be introduced for ATM transactions in the U.S.
  - MasterCard Oct. 2016; Visa Oct. 2017
  - All ATMs need to be EMV compliant
  - After October 2016/2017, FIs can hold ATM operators liable for fraudulent withdrawals and cash advances from debit and credit cards.
- Approximately $2,000 to upgrade an ATM to be EMV-capable (Aite)
  - Some ATMs will not take the upgrade for EMV and/or Windows (move from XP); 35k+ for a new ATM

Card Issuers & EMV

- Some U.S. card issuers began by issuing cards to frequent international travelers, corporate cardholders, T&E
- Only 1.5% of an estimated 1.2 billion payment cards in the US have an EMV chip
- Javelin predicts that, in Dec. 2015, only 29% of credit cards and 17% of debit and prepaid cards will be EMV-enabled.
  - At that time, Javelin predicts 53% of POS terminals will support EMV.

Card Issuers & EMV

- JPMC
  - First major card issuer to adopt chip-and-signature model for U.S. cards
  - Announced 2/25/2014 that it would begin issuing chip-and-PIN cards this year. Will others follow suit?
  - Expects most of its debit cards to be chip-enabled by EOY 2015
- BofA
  - Has been issuing chip credit cards (consumer, commercial, and corporate) since 2012
  - 9/30/2014: Announced it will begin issuing chip debit cards to new customers in Oct.; cards for existing accountholders issued as these cards expire or are replaced
  - Plans to have the majority of its cards converted by late 2015

Card Issuers & EMV

- Wells Fargo: “Testing chip technology with its debit cards and plans to issue them ‘on a broad scale’ in the coming year.”
- Citibank
  - Will begin issuing chip debit cards in 2015
  - All of its new consumer credit cards are issued with chip technology
  - Should have half of its portfolio of consumer credit cards chip-enabled by EOY 2014.
  - Most customers can go online or call customer service to request a chip credit card.

The U.S. Government & EMV

- 10/17/2014: President Obama signed an executive order committing the federal government to offer and accept EMV chip cards.
  - 5-6 million prepaid debit cards used for issuing government payments (e.g. Social Security; veterans benefits), will be reissued by Comerica Bank starting Jan. 2015.
  - 3 million cards issued to federal govt. employees will be replaced with EMV versions through the General Services Administration's SmartPay program.
  - All cards will be chip and PIN

Merchants & EMV

- Many merchants support elimination of signatures as a verification method in U.S., but Visa and MC will continue to support signature ("chip and choice").
- Merchants tend to favor PIN due to lower fraud rates than signature transactions.
- Visa and MC will also support transactions with no cardholder verification for low-value, low-risk transactions like payments at quick service restaurants (QSRs) and parking meters.
- "The ROI is simply not there without a PIN requirement. The signature card has by far has outlived its usefulness. It's not the mag-stripe that's the problem, it's the signature that's the problem."—Mark Horwedel, Merchant Advisory Group (MAG)

Merchants & EMV

- Only about 10% of the POS terminals in the U.S. are EMV-ready; mostly in “big-box” stores (Javelin)
  - Wal-Mart has turned on EMV acceptance at about 4,000 of its 5,000 stores
  - Javelin predicts 53% of POS terminals will support EMV in Dec. 2015.
- Wal-Mart, Home Depot and AMC Theaters all prefer PIN over signature

Merchants, Consumers & EMV

- Issue: Consumer Awareness
  - If a cardholder tries to swipe a chip card at a terminal as he would normally swipe a mag-stripe card, at a store where EMV acceptance has been enabled, the terminal prompts the cardholder to insert the card in the device so that it reads the chip.
  - Solution: Advertising and education by card networks and banks?
    - e.g., “Don’t remove your EMV card too quickly, but don’t leave it in the terminal either!
    - FRB Dallas Video

Issues (ASC X9)

- EMV's age
- EMV is a proprietary standard
  - Governments and other entities around the world are looking for open, non-proprietary standards
- International interoperability?
- Issuers, merchants, or processors object that they have not had a say in how the standard works or how it is being implemented in the U.S.
- Durbin Amendment: merchant choice when routing debit transactions
  - Resolved by "common application identifier" (AID)

Beyond EMV?

- Tokenization
- Point-to-Point Encryption
- 3DSecure (online)

Questions?

Matt Davies, AAP, CTP, CPP
Payments Outreach Officer
Federal Reserve Bank of Dallas
Phone: 214-922-5259
E-mail: matt.davies@dal.frb.org

Follow us on:

@DallasFed

DallasFed