Retail Law Conference

2016

RLC RETAIL LITIGATION CENTER

RILA
RETAIL INDUSTRY LEADERS ASSOCIATION
Educate. Collaborate. Advocate.

Data Compromise Issues:
Is Your Company in Shape To Deal with Banks & Card Networks?

CONSTANTINE | CANNON

Today's Presenters

- **Mike Williams, Executive Vice President and General Counsel, Staples, Inc.**
  - After 22 years as a trial lawyer in private practice in Los Angeles, California, became General Counsel of Sony Electronics for 8 years and has been with Staples since 2012.
- **Jeff Shinder, N.Y. Managing Partner, Constantine Cannon LLP**
  - Focuses on antitrust counseling and litigation. In the payments realm, has represented networks, merchants, and technology firms. Lead counsel representing a coalition of merchants that oppose a proposed settlement of a class action interchange case against Visa, MasterCard, and their major member banks, and represents multiple merchants in an "opt-out" action against them.
- **Steve Cannon, Chairman, Constantine Cannon LLP**
  - Active in payment card issues, including representing merchants and processors in litigation and before payment card brands with respect to claimed data compromises. Former General Counsel, Circuit City Stores, Inc.; former Deputy Assistant Attorney General, Antitrust Division; former Senate Judiciary Committee Counsel.

Themes from Last Year's Session

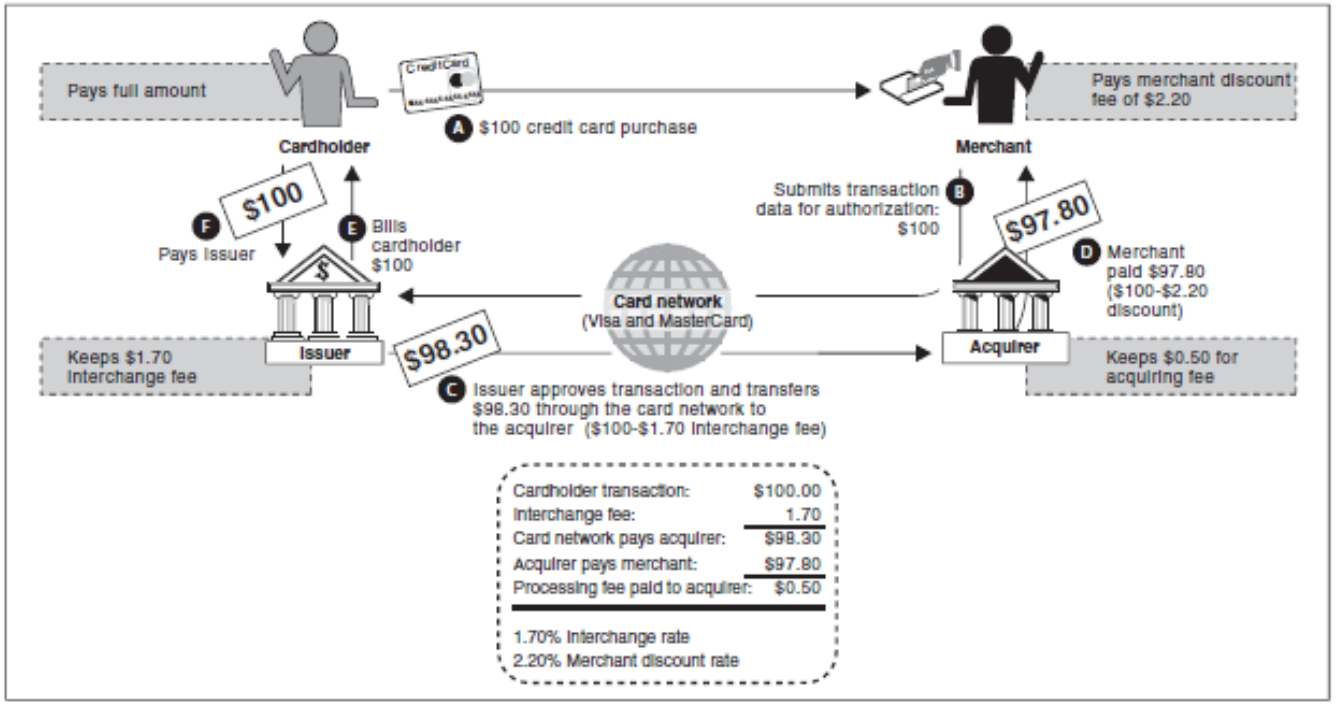
- The role of the EMV liability shift in increasing networks' control and revenue
- The battle of digital wallets
- Regulatory and legislative challenges
- The role of litigation: emerging scenarios

Today's Agenda

- Managing a Data Breach: A GC's Perspective
  - The Comprehensive Contingency Plan
  - The Role of the Brands and Your Acquirer/Processor
  - Executing the Plan
- The Evolving Liability Landscape
  - PCI and the EMV Transition are Entangled
  - A changing Role for Visa and MasterCard Recovery Mechanisms?
  - Emerging Merchant Litigation Issues

Networks Impose Their Security Rules and Assessments without Merchant Privity

Figure 2: Transfer of Fees in a Credit Card Transaction



Sources: GAO (analysis); Art Explosion (images).

Managing a Data Compromise: A GC's Perspective

What a Data Breach Looks Like to the General Counsel

When you’re up to your neck in alligators, sometimes you forget that your mission is to drain the swamp.

Confronting Multiple Simultaneous Investigations

- Internal
- PFI – Card Networks
- Law Enforcement – FBI, Secret Service, NY City DA
- State Attorneys General
- Office of Canadian Privacy Commissioners & Provincial Officials
- SEC
- FTC

The Importance of A Contingency Plan for a Payment Card Compromise

- Having to make it up as you go along puts the company, its customers, and shareholders at risk
- A comprehensive plan is a management and board responsibility
- Multiple corporate functions are involved
  - Legal
  - IT and IT security
  - Finance
  - Internal audit
  - Investor relations
  - Risk management
  - Corporate communications
  - Corporate security
  - Store operations
  - Human resources

The Role of Both Data Breach and Payments Industry Legal Expertise

- Most businesses will not have ongoing experience with arcane procedures invoked by networks when data breaches are suspected.
- "Data breach" counsel's practice may have dealt with state and federal enforcement agencies, class action litigation, not on the payment industry's regulations and procedures, which affect merchants and their payment processors in multiple dimensions
- Additionally, an understanding of payment industry dynamics may turn out to be crucial to a smooth investigation and minimizing potential liability.

Legal Maybe The Most Appropriate Incident Coordinator

- Legal's "day job" is rendering cross-functional advice
- Key aspects of the process have a legal nexus
  - Corporate governance- SEC responsibilities- "Blackout period"
  - Breach notification- state requirements and AG enforcement
  - The investigation: privilege for outside counsel and consultants, FTC investigation
  - Finance- Card processor and network contracts
  - Corporate communications- Consumer class actions
  - Potential liabilities- Insurance contracts

The Payment Card Industry

They are Judge, Jury, Executioner & Legislature all rolled into one.

Networks Can Impose High Costs When Breaches are Suspected

- Include PCI investigation costs, charge-backs, and systems of fines, penalties and assessments for PCI violations or claimed data breaches
  - May be unilaterally imposed by Visa and MasterCard based on "common point of purchase" and "incremental fraud" algorithms
  - Include Visa Global Compromised Account Recovery ("GCAR") and MasterCard Operational Recovery-Fraud Reimbursement ("OR/FR") mechanisms to compensate issuers for claimed fraud losses and card reissuance and account monitoring costs
  - Limited appeal rights to Visa and MasterCard dependent on acquirers
  - Collected through indemnification provisions (including "reserve account" rights) of merchants' agreements with their acquirers and processors
  - AmEx and Discover impose their assessments directly on merchants

The Card Networks Will Control the PFI Investigation

- Usually the networks, not your IT department will be the first to alert you to a potential compromise incident
- Visa and MasterCard, working through your processor or acquiring bank, will usually take the lead
- Each network's regulation's impose (slightly different) obligations on containing the breach, notifying the network as to potentially compromised cards, and retaining a PCI-approved Forensic Investigator ("PFI")
- Imposition of fines for "non-cooperation"

Remember What the Card Brands Want

- Dates of intrusion (may be different than date of exfiltration)
- Credit Card numbers
- Number of cards exposed
- Whether remediation has taken place
- To prove your PCI non-compliance
- $$$$ in the form of reimbursements, general fines & fees

The PFI is "Independent"

- You pay for the PFI
  - But networks may review your choice of PFI to make sure it has no conflicts due to prior work for you (e.g., an annual PCI assessment)
  - The PFI has an ongoing relationship with the networks; the merchant doesn't
- You get to comment on draft PFI reports
  - But the PFI retains the right to incorporate your comments or not
  - PFI must certify that conclusions are its own
- The PFI report is proprietary
  - But is provided to all the networks, who use it as a basis for their liability assessments

Retaining Your Own Additional Forensic Investigator May Be Wise

- Retained by counsel to maximize privilege claim
  - Consultant providing advice in contemplation of litigation
  - Serving as potential non-testifying expert under Rule 26(b)(4)(D)
- Can provide a more comprehensive or tailored investigation than the PFI
- Can provide a second opinion (through counsel) with respect to the PFI's findings, including suggestions for changes

Lawyers Should Participate in Discussions With Networks

- Networks usually ask for weekly status conferences on progress of PFI investigation, until it is complete.
- Networks will ask to talk to PFI after report is issued; these calls may impact their liability calculations; they may have follow-on questions—and the interests of the networks may differ
- There also will be an opportunity to appeal Visa and MasterCard liability determinations (via processors); AmEx and Discovery may provide the opportunity for direct settlement negotiations

Keep Management and the Board Updated

- Dependent on the size of the breach, it may have a reportable impact on a firm's finances
- The General Counsel may have to ensure that officers are aware of the investigation and help mediate issues of responsibility and a path forward

THE EVOLVING LIABILITY LANDSCAPE

The PCI Process Is Controlled by the Networks

- The Payment Card Industry Security Standards Council is controlled by Visa, MasterCard, American Express, Discover, and JCB
  - Issues the PCI Data Security Standards and the PCI Payment Applications Standards
- Unlike the formal standards-setting bodies, there is no attempt to achieve a "consensus" of relevant participants, including merchants
  - Yet card issuers and public officials treat the PCI requirements as if they were the product of a true standards-setting organization with participants having due process rights

The Networks have Intertwined PCI and the EMV Transition

- Networks use the PCI/breach liability process to coerce merchants to transition to the vulnerable chip and signature EMV approach
- The October 1, 2015 counterfeit fraud liability shift has been a costly disaster that reinforced Visa and MC efforts to undercut Durbin Amendment routing of PIN debit to protect there debit market dominance
- Visa and MC waive annual PCI compliance certification if 75 percent of card volume is from EMV terminals with dual contact/contactless-NFC interfaces, yet the EMV transition would not have prevented export of data major breaches

The EMV Transition May Affect Network Data Breach Assessments

- Visa and MasterCard provide a safe harbor from GCAR and OR/FR assessments if 95 percent of a merchant's card-present transactions are made through EMV terminals
- But merchant obligations to card networks to investigate, minimize the impacts of, and remediate any breaches that do occur would remain

Dissatisfaction with Network Recoveries Has Led to Issuers Suing Merchants

- Recent credit union, small bank class actions to recover claimed losses from data compromises
  - Settlements in Target litigation: in part based on Minnesota statute that authorized issuers to recover losses above network reimbursements
  - The Home Depot's motion to dismiss was denied on negligence, negligence per se claims based on claimed violation of FTC Act, state "little FTC" acts (interlocutory appeal motion pending)
  - Issuers in *Schnuck's Market* last week filed an amended complaint based on *Home Depot* ruling, alleges PCI, network rule, FTC Act, violations constitute negligence, negligence per se

MasterCard is Telling (Smaller) Issuers to Accept its Black Box Formula Or Sue Merchants

- February 2016 amendment to its Security Rules
  - Requires issuers participating in the "reimbursement component" of data compromise program (OR/FR) to agree to release acquirers and merchants from further financial liability
  - But permits issuers to opt-out of OR/FR annually and to pay reduced fees to MasterCard, gaining right to sue
  - An issuer also may reject a specific recovery and gain right to sue merchant
- MasterCard reserves the right to cancel OR/FR mechanism if there is "insufficient participation" in the mechanism

Emerging Merchant Litigation Issues

- FTC use of PCI compliance as a standard for merchant liability under FTC Act section 5
  - Court-approve settlement required Wyndham's compliance with PCI standards or successor standards agreed to by all the card networks
  - Third Circuit ruled in 2015 that FTC Section 5 enforcement action against Wyndham Hotels for a card breach was within Section 5's scope
- Potential ability of merchants to attack issuer (class) actions based on realities of payment networks
  - Can issuers suffer damages if they have already been compensated for risks of payment system through interchange fee payments?
  - As members of Visa and MasterCard networks, can issuers claim losses that resulted from networks' decision to retain insecure magstripe technology long after rest of world move to chip and PIN?

How To Reach Us

- **Mike Williams:**
  - michael.williamsgc@staples.com
  - 508-253-0637
- **Jeff Shinder**
  - jshinder@constantinecannon.com
  - 212-350-2709
- **Steve Cannon**:
  - scannon@constantinecannon.com
  - 202-204-3502

APPENDIX

Glossary of Common Data Security and PCI Terms

- **Acquiring bank** The Bank used by a merchant to processes payment card transactions. For example, an acquiring bank is Bank of America Merchant Services (BAMS)
- **Issuing bank** The Bank that issues payment cards to customers, for example Citibank, Wells Fargo, Citizens, and HSBC
- **Payment card brand** Visa, MasterCard, Discover, Amex, etc.
- **CPP** Common Point of Purchase – a location where credit cards may have been compromised; for example, a bank/brand will identify where a credit card that was fraudulently used was last used legitimately; if a group of fraudulent credit card transactions traces back to a common last location of legitimate use, the location will be deemed a "CPP"

Glossary, cont'd

- **CSC** Card security code (CSC), sometimes called card verification data (CVD), card verification number (CVN), card verification value (CVV or CVV2) are different terms for a security feature for "card not present" payment card transactions instituted to reduce the incidence of credit card fraud. The codes have different names by card brand: MasterCard – card validation code ("CVC2");Visa – card verification value ("CVV2"); Discover – card identification number ("CID"); American Express – "CID" or "unique card code"; and Debit Card – "CSC" or "card security code"
- **Firewall** A device or program that limits network traffic according to a set of rules about what traffic is or is not authorized
- **Forensic image** An exact copy of the content and format of a digital storage device (such as a disk)
- **PAN** Primary Account Number is the numerical value stored in Track 1 and/or Track 2 on the Payment Card and it is usually the credit card number.

Glossary, cont'd

- **PCI standards** Payment Card Industry standards developed by the payment card brands that specify security requirements for handling payment card information
- **PFI** PCI Forensic Investigator – Payment card brands require a merchant to engage a PFI to investigate data security incidents and/or CPP reports and report the cause and extent of any data security incident to the banks.
- **Track Data** Magnetic stripes on payment cards are divided into three tracks of data which are encoded directly to the magstripe. Only Track 1 and Track 2 are actively used in payment card processing. Track 3 is rarely used and may not always be present on a card. Both Track 1 and Track 2 contain enough basic information for processing payment card swipes. Most card readers will be able to read both Track 1 and Track 2 data, in case one of the tracks has become unreadable.