Payment Cards Center

Federal Reserve Bank of Philadelphia

Update

A newsletter published by the Payment Cards Center, providing meaningful insights into developments in consumer credit and payments

Spring 2009

From the Director

Peter Burns, Vice President & Director

Peter Burns

Welcome to this edition of *Update*, a periodic publication of the Payment Cards Center highlighting recent activities. Also available on our website, *Update* complements the more complete content at www.philadelphiafed.org/payment-cards-center/publications/.

I would like to take this opportunity to introduce the new director of the center and thank all of our readers for their interest and support during my tenure. As many of you know, I came to the Philadelphia Fed some eight years ago to establish a research initiative focused on consumer credit and payments. It has been an exciting and personally rewarding time for me, and I am grateful for the support from center and Bank staff as well as from you, our partners from industry, academia, and the policy community. As I look back, I think we can be collectively pleased that we contributed to a greater understanding of central business issues and helped to inform relevant policy. With the center reaching a certain maturity and gaining in influence, I am ready to move on to new challenges.

I move forward confident that we have a strong team in place and new leadership that will not only ensure that there is continuity in the center's activities but also add new and relevant perspectives. I am very pleased that Bob Hunt has agreed to become the center's director. Bob brings with him an accomplished background in research in many of the areas important to the center. A more comprehensive description of his background and interests follows this introduction. I would only note that I have had the pleasure of working closely with Bob since the center's inception and have every confidence that he will serve your interests well and elevate our agenda to new levels.

Mission Statement

The mission of the Payment Cards Center is to provide meaningful insights into developments in consumer credit and payments that are of interest not only to the Federal Reserve but also to the industry, other businesses, academia, policymakers, and the public at large. The center carries out its mission through an agenda of research and analysis as well as forums and conferences that encourage dialogue incorporating industry, academic, and public-sector perspectives.

In This Issue:

This issue of *Update* also features brief summaries of several recent papers authored by center analysts as well as a summary of last year's payment card fraud conference. Complete versions of these documents are available on our website. As an aside, I would encourage you to visit the site, which has recently undergone a substantive redesign and upgrade. Let us know what you think.

The several documents reviewed later in *Update* reflect the continuation of various research themes within the center. Both Philip Keitel's paper, "The Laws, Regulations, Guidelines, and Industry Practices That Protect Consumers Who Use Gift Cards," and Ann Kjos's paper, "New Prospects for Payment Card Application in Health Care," extend the center's examination of the emerging market for prepaid card payments. Both papers have been well received and cited in various trade publications. The second paper of Philip's reviewed in this issue, "Legislative Responses to Data Breaches and Information Security Failures," and Susan Herbst-Murphy's summary of our conference on "Maintaining a Safe Environment for Payment Cards: Examining Evolving Threats Posed by Fraud," reflect the center's continued focus on the issues of fraud, identity theft, and other threats to the safety and integrity of our modern electronic payment systems.

As always, we invite your thoughts, comments, and suggestions on how we might increase the effectiveness of our efforts.

New Center Director Appointed

When the Payment Cards Center was established in 2000, its mission was to be a source of knowledge and expertise on this important segment of the financial system, which includes credit cards, debit cards, smart cards, stored-value cards, and similar payment vehicles. To accomplish this, part of the plan was to develop relationships with

Bob Hunt

others in the Bank whose work would support this mission. At that time Bob Hunt was identified as someone who could be important to the center. As a senior economist in the Bank's Research Department, his research focused on consumer payments, consumer finance, and the economics of innovation. His work includes studies of the dynamics of the consumer credit reporting industry, credit counseling organizations, the collections industry, and antitrust issues in consumer payment networks.

Early on, Bob's working paper on consumer credit reporting in America was one of the first to be added to the Payment Cards Center's website, to be followed by others, such as "An Introduction to the Economics of Payment Card Networks."

In 2002 the Payment Cards Center and the Research Department sponsored their first conference together, with Bob taking the lead. Since then, Bob has continued to take the lead on our co-sponsored conferences, with our fifth joint conference scheduled for September 2009.

In the seven years Bob has worked with the center he has helped guide its research activities in an informal advisory role to the center's director. With such a strong presence in the work of the Payment Cards Center, it was no surprise when he was selected to succeed Peter Burns as the center's director.

In the seven years Bob has worked with the center he has helped guide its research activities in an informal advisory role to the center's director.

Bob joined the Payment Cards Center as an assistant vice president in January 2009. In April 2009, he became the director of the Payment Cards Center with responsibility for managing the center and its research agenda.

He received a Ph.D. in economics from the University of Pennsylvania and a B.A. in political science and economics from Butler University.

Before he joined the Bank in 1998, Bob worked as an associate analyst for the U.S. Congressional Budget Office. Prior to attending graduate school, he was an industry risk analyst for Bank One, Indianapolis.

The Laws, Regulations, Guidelines, and Industry Practices That Protect Consumers Who Use Gift Cards

Expanding on the center's prepaid card research, Philip Keitel discusses consumer protections available to gift-card users in his recent paper "The Laws, Regulations, Guidelines, and Industry Practices That Protect Consumers Who Use Gift Cards."* This paper specifically considers the protections for the two types of prepaid gift cards: "closed-loop" and "open-loop." Closed-loop cards are typically sold by individual retailers, serviced by those retailers (or their agents), and function only at that particular retailer's locations. Open-loop cards are issued by financial institutions, operate over debit or credit networks, carry a network logo, and can be used at any retail location that displays the payment network logo. In describing consumer protections for gift cards, Keitel cites several sources, including state statutes, Federal Trade Commission decisions, financial industry regulatory guidelines, and past interviews with payments industry experts.

Closed-loop cards account for both the majority of gift cards sold and the majority of dollars loaded onto gift cards. While there are presently no federal laws or regulations that protect consumers who buy and use these gift cards, approximately 40 states and the District of Columbia have enacted legislation designed to protect purchasers of gift cards. Although the specific laws vary, they generally deal with issues related to fees (issuance fees, service fees, dormancy charges for nonuse), the length of time before cards may expire, and the disclosures that must be made to consumers. A number of states also apply their abandoned property laws to unused balances on closed-loop gift cards, requiring that unclaimed balances revert to the state treasury after a defined period of time. The amounts involved are not trivial, with some estimates suggesting that unused gift card balances are in the multibillion-dollar range. While there are similarities among state laws, there are also important differences. For example, provisions that stipulate the amount of time that must pass before cards may expire were found to range from one to seven years.

In addition to state laws, state attorneys general have taken action against gift-card issuers and program operators. In 2002, for example, Home Depot changed its national policy regarding lost or stolen cards after then-Attorney General Eliot Spitzer questioned some of the retailer's gift-card program practices. As a result of this agreement, consumers who report lost or stolen Home Depot gift cards and provide proof of purchase can request deactivation and replacement of

*Available on the center's website at: http://www.philadelphiafed.org/payment-cards-center/publications/discussion-papers/2008/D2008JulyGiftCard.pdf.

the original card. Today, virtually all gift-card programs offer similar protections.

The Federal Trade Commission (FTC) has also been active in protecting consumer gift cards. In two separate cases in 2007, the FTC ruled that Darden Restaurants Inc. and Kmart Corp. were guilty of "unfair or deceptive practices" involving their gift-card programs. Specifically, it was found that disclosures at the time of purchase did not adequately and clearly define dormancy fees that went into effect after the cards had not been used for some time. The gift-card issuers were ordered to make changes to their disclosure practices and take ameliorative actions. As a result, many gift-card programs now generally follow these FTC-ordered disclosure practices.

While there are presently no federal laws ... approximately 40 states and the District of Columbia have enacted legislation designed to protect purchasers of gift cards.

The other type of gift card discussed in Keitel's paper is the open-loop, or network-branded, gift card. While smaller in volume than closed-loop retail gift cards, open-loop cards represent an important and growing segment of the market. Unlike retail gift cards, open-loop cards are issued by financial institutions that are subject to federal regulations. These regulations are principally issued by the Office of the Comptroller of the Currency (OCC) and the Office of Thrift Supervision (OTS). Having generally issued similar rules related to disclosures and substantive practices for operating gift-card programs, the OCC and the OTS distinguish between the purposes behind particular types of disclosures – recognizing that certain information is relevant to the purchaser's decision making, while other information is essential to the user and should be "passed on from the gift card purchaser to the gift card recipient."

Another source of consumer protection for open-loop gift cards comes from rules established by the card networks whose brands adorn the cards. For example, in some instances networks extend consumer protection policies developed for credit and debit card users to open-loop gift-card holders. Two such critical policy extensions relate to "zero liability" and chargebacks. Under the zero liability rule, networks require issuers of network-branded gift cards under certain circumstances to re-credit consumers within five business days for any losses suffered as a result of reported unauthorized transactions. Under chargeback rules, issuers are able to charge back to retailers transactions deemed to have been faulty. While this protection is sometimes extended to open-loop gift-card holders, Keitel cites interviews in which card issuers suggest that there are differences in how aggressively chargeback remedies are extended – often depending on the nature of the cardholder relationship.

The applicability of state laws (including state gift-card laws, abandoned property laws, and various other state laws) to open-loop gift-card programs offered by nationally chartered financial institutions is characterized by Keitel as a dynamic and evolving area of law. While some state statutes specifically exempt gift-card products issued by these financial institutions from their purview, others specifically target these issuers. This general issue – whether state consumer protection laws aimed at gift-card consumers apply to open-loop cards issued by federally regulated financial institutions – has been at the heart of several actions brought by state attorneys general. While Keitel notes that appellate court decisions have helped clarify elements of the debate, including whether federal law preempts state law here, the general question has not been completely resolved.

Today's gift card programs, both closed-loop and open-loop, often provide substantial consumer protections as a result of actions taken by state legislatures, state attorneys general, federal agencies, financial institutions, and payment networks. The increasing use and high consumer satisfaction levels associated with gift cards are likely to be, at least partly, the result of consumers' comfort with these protections. However, this minimal risk feature of gift cards may change as innovation in payments continues. Should new gift-card models expand beyond the original low-value, short-lifetime concept, the need to address new consumer protection issues will likely follow.

New Prospects for Payment Card Application in Health Care

Consumers' use of payment cards for making health-care payments has been relatively limited. According to McKinsey & Company, approximately 80 to 90 percent of health-care expenditures are paid by cash or check. In her paper "New Prospects for Payment Card Application in Health Care,"* Ann Kjos explores several reasons for the slow adoption of payment cards to date and discusses four specific trends and developments that may lead to increased growth in the future.

Health-care payments in the United States are overwhelmingly concentrated among government and business entities. Nevertheless, direct consumer payments – estimated at around $269 billion in 2007 – are substantial. While cash and

* Available on the center's website at: http://www.philadelphiafed.org/payment-cards-center/publications/discussion-papers/2008/D2008NovemberHealthCareCardApplication.pdf.

check have been the traditional form of payment, credit and debit card terminals are becoming more common in doctors' offices and hospitals. At the same time, payment innovators are also focused on several specific health-care programs that appear to offer particular opportunities for payment card applications. These programs fall under the rapidly growing segment of consumer-directed health care: flexible spending accounts (FSAs), health reimbursement accounts (HRAs), and health savings accounts (HSAs). Individuals with an FSA or HRA can use a payment card to access funds set aside for health-care expenses, eliminating the need to submit receipts for reimbursement. The most recent program innovation, the HSA, was designed to incorporate a payment card application. With an HSA, individuals with health-care plans that have high deductibles can make tax-deductible contributions to their accounts, saving for qualified medical and retiree health expenses that can be accessed with a debit card.

Individuals with an FSA or HRA can use a payment card to access funds set aside for health-care expenses, eliminating the need to submit receipts for reimbursement.

Early expectations for card-based spending centered on these relatively new programs were extremely high. However, actual use of payment cards for these programs was estimated at only 3 percent of total consumer out-of-pocket expenses for 2007. More specifically, spending with FSA, HRA, and HSA cards accounted for $5 billion, $255 million, and $2.5 billion, respectively. In general, consumer adoption of these health-care options has been much slower than originally anticipated. According to Metavante Corporation, there were fewer than 20 million FSA, HRA, and HSA enrollees in 2005. As a result, a number of early payment card entrants into the market, including American Express and Discover, have cited limited market potential as a reason for cancelling or pulling back on their initiatives.

In addition to slow growth in these targeted programs, another impediment to card use has been the complex nature of health-care payments and the challenge of adapting traditional card payment processes to this different environment. Among the several examples discussed in the paper is the impact that the complexity of product pricing has on this payment card application. While the price of a good is readily established in a retail merchant environment, the price of a health-care service is often not available at the point-of-sale and is subject to different deductibles or co-payment structures. Moreover, transactions are often connected over time as part of an ongoing treatment, and payments are subject to complex adjudication rules. While payment card providers are developing solutions to these challenges, progress has been slower than anticipated.

Nevertheless, Kjos believes there is good reason to expect that these programs and associated payment card applications may soon experience more significant growth. She discusses four specific trends and developments: (1) a general shift away from employer-provided health care to card-friendly consumer-directed health-care plans (CDHPs), (2) an expansion of HSAs in particular, (3) a move toward using debit and prepaid card applications to address limitations in traditional paper-based FSA and HRA environments, and (4) new IRS regulations that address important impediments to expanding CDHPs and payment card applications.

HSAs offer a number of attractive features to employees, and their card-based payment structure is expected to particularly attract the interest of payment providers.

Spending on health-care services is growing faster than the country's gross domestic product. Due to this rapid rise in overall health-care costs, many employers have been shifting away from employer-provided health-care plans and toward CDHPs. As this trend continues, and perhaps accelerates, the underlying payment patterns will shift toward a greater mix of consumer-directed payments. This, in turn, is expected to generate opportunities for payment card providers supporting FSA, HRA, and HSA programs.

Despite slow growth to date, many observers believe that as employers adopt or shift to CDHPs, HSAs stand especially to benefit. HSAs offer a number of attractive features to employees, and their card-based payment structure is expected to particularly attract the interest of payment providers.

The third factor that Kjos expects will spur increased card use in consumer-directed health-care payments is the special advantages that cards have in FSA and HRA programs. While these programs were originally structured on the basis of paper-based payment reimbursements, Kjos argues that the use of prepaid or debit cards can make such programs more attractive and increase adoption. An employee with an FSA that is not linked to a card encounters a "double payment" problem. First, the employee pays when money is taken from his or her paycheck to fund the FSA and, second, when making the health-care purchase. After the purchase, the employee needs to submit receipts to receive reimbursement. When an FSA is coupled with a debit or prepaid card, the employee makes only one "payment," which occurs when the account is funded. The health-care purchases made with an FSA card are deducted directly from the account, eliminating the second payment and the whole reimbursement process. Although an HRA does not involve the employee paying twice, since it is funded by the employer, the same cumbersome reimbursement process exists. Thus, the use of a debit or

prepaid card addresses the limitations of the cash and check payments for both accounts.

The final factor discussed is a recent IRS ruling that is expected to greatly increase the attractiveness of card-based payments and by extension the adoption of related CDHPs generally. Although the IRS introduced the option of electronic substantiation of eligible purchases for CDHPs in 2003, many purchases still ended up requiring additional cumbersome manual processes, particularly at nonmedical merchants such as supermarkets, grocery stores, discount stores, and wholesale clubs. As a result of a follow-up ruling in 2006, a far simpler, card-friendly alternative was authorized. While it is too early to tell how effective the rule change will be, the intuition is that making payment card alternatives more attractive should expand their adoption by consumers.

Despite the fact that growth of card-based health-care payments has fallen considerably short of earlier expectations, Kjos argues that four specific developments and evolving trends may be expected to accelerate adoption rates. At the same time, there is reason to urge some caution in interpreting the potential impact of these developments. The four factors discussed generally address structural or process barriers that have limited program growth and payment card application. The role of consumer behavior in health-care choices, however, is not explicitly examined in this analysis. Based on the dramatic differences between historical growth forecasts and actual results highlighted in the paper, it is certainly possible that some of this disjunction may be due to undervaluing the role of consumer behavior in this area. While the paper argues that new product development and market trends all support more optimistic growth forecasts, it also suggests that more research into consumer behavior and attitudes is needed.

Legislative Responses to Data Breaches and Information Security Failures

A 2007 government analysis noted that in the previous two years over 1,000 data breaches were reported in the United States and that the rate at which breaches were occurring appeared to be increasing. Because these breaches, which involve the theft of personally identifiable information such as name, address, Social Security number, and credit card data, are closely related to payments fraud and identity theft, the Payment Cards Center hosted a workshop on July 23, 2008, to discuss how Congress and various state legislatures have responded.

The workshop was led by Diane Slifer, J.D., M.B.A., who has frequently presented at forums on data security and has represented clients in matters related to data breaches. In his paper "Legislative Responses to Data Breaches and Information Security Failures,* Philip Keitel provides an overview, based on Slifer's presentation and his own research, of several laws that have been enacted to address issues related to data breaches and the general protection and handling of sensitive consumer information.

The FACT Act requires federal banking agencies to make certain that information taken from consumer reports and used for a business purpose is disposed of properly.

One of the laws, the Gramm-Leach-Bliley Act (GLB Act), was enacted by Congress in 1999. The GLB Act includes three principal provisions intended to protect consumers' personal financial information held by financial institutions. The first provision, the financial privacy rule, calls for financial institutions to establish and communicate policies concerning their use of the personal financial information of consumers and to afford consumers control over how this information is shared with others. Second, the GLB Act includes a safeguards rule that requires financial institutions to have a security plan in place to protect the confidentiality and integrity of personal consumer information. The third and final rule encourages institutions covered by the GLB Act to implement safeguards against "pretexting" — that is, attempting to gain access to the personal information of another by creating a false scenario.

In addition to the GLB Act, Slifer discussed rules on protecting consumer data and preventing identity theft contained in the Fair and Accurate Credit Transactions Act (FACT Act) of 2003. One such rule requires federal banking agencies to make certain that information taken from consumer reports and used for a business purpose is disposed of properly. Another FACT Act rule, known as the receipt truncation provision, requires those who accept credit cards or debit cards for business transactions to print no more than the last five digits of the card number or the expiration date on receipts. Under the FACT Act's "red flag" provisions, banking institutions must establish policies and procedures that help prevent identity theft. For example, debit or credit card issuers must assess the validity of a change of address if it is followed shortly by a request for a new card. Finally, the address discrepancy provisions in the FACT Act require entities that request consumer credit reports to develop reasonable policies and procedures to

---

*Available on the center's website at: http://www.philadelphiafed.org/payment-cards-center/publications/discussion-papers/2008/D2008DecemberLegislativeResponsesToDataBreaches.pdf.

respond to situations where an address reported differs from one already in a consumer's credit report.

Today, Social Security numbers (SSNs) are broadly disseminated in many environments where they serve as personal identifiers, something that was not foreseen when the system was created in 1936. As a result, they have become a favorite target for cyber criminals who use others' SSNs to create false identities or to assume another individual's identity for the purpose of committing financial crime. In response, more than 42 states have, since 2005, enacted some form of law that regulates the use of SSNs or mandates a particular method for protecting the information. While there is some variation in these laws, the most common provisions include prohibiting companies from printing SSNs on identification cards or other materials; restricting the intentional communication of the numbers, whether by mail or public posting; and requiring that when used, the numbers be truncated or otherwise modified. As discussed in the paper, state laws related to SSNs have often had a significant effect on traditional business practices. One government report found that the sharing of the numbers among commercial partners and third-party vendors is common and often defined in contract language and in long-established business practices.

Finally, the paper addresses laws pertaining to notification required after a data breach has occurred. As of July 2008, 48 states (all but New Mexico and South Dakota) possessed a law concerning notification after a data breach or had such a bill pending before their legislatures. These laws generally require notification of consumers, state agencies, or other parties when unencrypted personal information held in some manner by an organization is acquired or accessed by an unauthorized person. However, the provisions of these laws vary widely from state to state. For example, some states require notification only when there is an identifiable risk of harm to a consumer, while others require notification when any relevant information is believed to have been accessed by an unauthorized party, irrespective of possible harm to consumers. As this example illustrates, diverse state-by-state requirements present real compliance challenges.

For more than a decade, federal and state legislators have tried to create an improved environment for private consumer data and to help protect consumers whose personal information has been compromised. Despite these efforts, policymakers and industry participants still face many obstacles to preventing and responding to data breaches. In today's technological environment, where wireless devices and remote access are commonplace, fraudsters can be expected to attack data security systems in new and unanticipated ways. One lesson to be drawn is that efforts to protect against the risk of data breaches represent daunting and continuing challenges for both industry participants and policymakers.

Payment Cards *and Evolving Threats Posed by Fraud*

On April 23 and 24, 2008, the Payment Cards Center and the Electronic Funds Transfer Association (EFTA) jointly hosted a conference titled "Maintaining a Safe Environment for Payment Cards: Examining Evolving Threats Posed by Fraud."* One goal of the conference was to provide a broad examination of card fraud by including a range of payment system players. Thus, there were panels representing consumers, issuers, networks, and merchant acquirers. The intent was to frame discussion of payment card fraud in such a way as to include these various perspectives. While the full conference summary is organized around these panels, this short synopsis focuses on key themes identified in the summary document.

The conference began with the cohosts, Peter Burns of the Payment Cards Center and Kurt Helwig of the EFTA, introducing keynote speaker Jon Greenlee, an associate director of the Division of Banking Supervision and Regulation with the Federal Reserve's Board of Governors. Specifically addressing regulation, Greenlee described how the Federal Reserve and other bank regulators have paid increasing attention to the issues of fraud and operational risk in retail payment systems. In response to the growing size and scope of retail payment systems, policymakers have moved beyond their traditional focus on wholesale payment systems. They want to ensure that there is continued confidence in the safety and integrity of payment systems, especially as payments move to electronic platforms. Greenlee argued that should data breaches and related fraud or identity theft threaten consumer confidence in electronic payments, the system as a whole could be threatened. Furthermore, he noted that innovations in payments that lead to greater consumer convenience may also create new risks. The growing involvement of third-party participants in consumer payments may also affect risk profiles as more sensitive information resides outside of a bank's "four walls" and thus creates new challenges for banks and their regulators.

After Greenlee's opening remarks, Peter Burns introduced and moderated the conference's first panel, which offered an overview of key elements in the dialogue about payment card fraud and a context for the next day's panels. Already some of the main themes of the conference began to emerge. For example, Richard Parry of JPMorgan Chase argued that more holistic efforts are needed across the entire banking organization because of cross-channel fraud vulnerabilities. Paul Tomasofsky of Two

*The complete conference summary, by Susan Herbst-Murphy, is available at: http://www.philadelphiafed.org/payment-cards-center/events/conferences/2008/PCCAprEvolvingThreatsFraud.pdf.

Sparrows Consulting raised concerns about the vulnerability that may exist in the United States as other parts of the world adopt chip and PIN cards. Avivah Litan of Gartner Inc. emphasized the sophistication of today's payment card fraudsters. The changing nature of fraud, therefore, requires new and collaborative approaches in order to develop effective solutions.

The second day of the conference began with welcoming remarks from the Philadelphia Fed's president, Charles Plosser. Calling attention to the increasingly complex security challenges that exist in today's high-technology and electronic-data-intensive card payment environment, President Plosser observed that while advances in electronic payments enable efficiency and welfare-improving outcomes, these modern payment systems could expose sensitive data to theft "in quantities that would not have been available in previous eras." The data thieves are well-organized and professional and are part of well-funded criminal groups. They operate domestically and internationally and use advanced technology in their efforts. Plosser emphasized the importance of consumer confidence in payment systems and its dependence on a secure and safe environment. Thus, it is the obligation of all who touch sensitive information to join in efforts to ensure its safety.

In order to secure such data, Plosser called for the cooperation of otherwise competitive market participants, in conjunction with law enforcement and data security experts. Historically, the industry has been effective at managing fraud due in large part to just such collaboration. Further encouraging cooperation, Plosser observed that "the card payment system's integrity relies upon a set of interdependencies and a shared responsibility." He added that the system's divergent constituencies cannot overcome the battle by operating independently. Since its inception, Plosser noted, the Payment Cards Center has provided such collaborative opportunities by bringing dif-

Setting the stage panel: James Brown, University of Wisconsin; Paul Tomasofsky, Two Sparrows Consulting; Richard Parry, JPMorgan Chase; and Avivah Litan, Gartner Inc.

fering perspectives together in a search for common solutions. He concluded by challenging conference attendees to work together constructively during the day's dialogue on maintaining a safe environment for payments.

The remainder of the conference consisted of four panel-led discussions, each focusing on one of the four players in the payment card structure: consumers, issuers, networks, and merchant acquirers. A number of the common themes that emerged from these discussions are highlighted below.

Reconsideration of Chip-Card Technology

For the past two decades, the common wisdom has been that smart cards are "a solution in search of a problem." Based on opinions voiced at the conference, there seems to be a recognition that fraud may well be the problem solved by chip- and PIN-based smart cards. As more of the world becomes chip-card enabled, fraud has migrated to regions dependent on magnetic-stripe technology. In addition, a participant suggested that the divergence of mag-stripe technology in the U.S. and chip cards in other parts of the world poses challenges to global interoperability. Despite the enthusiasm of many for a chip and PIN solution, others pointed to the perhaps prohibitive cost of such an overhaul of system infrastructure. In addition, some questioned whether, instead, a new approach that addresses card-not-present and other chip and PIN limitations is needed. While not discussed in detail, end-to-end encryption was noted as one such possibility.

Adoption of Payment Card Industry Data Security Standards (PCI-DSS)

Merchants have accelerated their compliance with PCI requirements for data security that were established by the major card networks. There was a general consensus that this was a critical measure that calls for commonsense data security practices. At the same time, some argued that requirements should reflect the differing risk profiles of large and small merchant categories. Lastly, a participant contended that PCI compliance is not a

Network panel: Ron Congemi, EFTA; Russell Schrader, Visa Inc.; Jodi Golinsky, MasterCard Worldwide; and Mark O'Connell, Interac Association and Acxsys Corporation.

"one and done" solution but is instead an ongoing process requiring continual vigilance and adaptation.

Sophisticated Fraud Rings Employing Advanced Technology

A number of panelists emphasized that the changing nature of fraud and the technologies employed have heightened the threat level for industry participants. Today, fraudsters are often organized professionals using much of the same technology employed by legitimate industry. They frequently employ variations of models used in the legitimate business world to carry out their activity. They use databases that mimic credit bureaus, match and append data elements in ways that emulate legitimate data aggregators and sell the stolen information, and employ time-sharing techniques used by lawful enterprises. One participant observed that these sophisticated fraud rings operate in a kind of illegal "parallel universe" that mirrors the legitimate payment industry.

Fraud Seeks a Path of Least Resistance

A related theme highlighted throughout the discussion was that fraud mitigation is a reactive process, with criminals learning to avoid secured access points and targeting weaker products, channels, and geographies. While this dynamic has always been a reality in payment fraud, a number of participants argued that the proliferation of products, access channels, and the globalization of electronic payments have dramatically increased the mitigation challenges. Also, because thieves maneuver across products and channels to perpetrate fraud, and multiservice households expect protection against fraud across the entire relationship, the nature of mitigation strategies is changing. Instead of traditional silo approaches, a number of full-service financial institutions are altering their fraud management structures to cross internal product, channel, and platform silos.

A related theme highlighted throughout the discussion was that fraud mitigation is a reactive process, with criminals learning to avoid secured access points and targeting weaker products, channels, and geographies.

Growth, Complexity, and the Need for Greater Cooperation And Coordination

Payment card usage has become both more ubiquitous and more complex. E-commerce and electronic banking have generated a proliferation of end-points. The increased electronification of information makes the capturing of data vulnerable while the information is "in transit" or "at rest." As these and other factors were discussed, a general conclusion arose that we must avoid assuming that there is a "magic bullet" that will ameliorate the problem. Rather, the industry must continue to mitigate fraud with multifaceted and dynamic solutions and the cooperation and collaboration of all parties handling vulnerable information.

The Role of Consumers in Mitigating Fraud

In recent years, identity theft and retailer data breaches have been highly publicized in the press. This has raised awareness among the general public about the risks that can affect individuals and, some argued, could lead to a loss of consumer confidence in electronic payments. A participant noted that while consumers often indicate that they want to be involved in securing their information, they do not always act in their own best interests; for example, they may respond to phishing attacks by providing their personal information. Networks, acquirers, and card issuers would all welcome consumers taking part in fraud-prevention strategies, but zero liability protections and other factors pose challenges to achieving this goal. While there was general agreement that enlisting consumers in fighting fraud is an important goal, participants acknowledged that little progress has been made to date.

Merchant acquirer panel: Marc Abbey, First Annapolis Consulting; Robert Carr, Heartland Payment Systems; Michael Herman, Chase Paymentech Solutions; and Donald Boeding, Fifth Third Bank.

Suggestions for research and experimentation that might encourage consumer involvement included more effective education, development of positive incentives for proactive behavior, and more emphasis on technological applications such as text message alerts and other real-time information flows.

While discussion at the conference did not center on specific proposals, it did explore a number of critical insights and identify new directions for further research. As several participants noted, an element key to a productive exchange of views was the conference's inclusion of the multiple perspectives represented by payment system participants. This reflected a general conclusion that successfully combating fraud in the modern payment card system cannot be accomplished in separate silos across the payment chain. Ultimately, successful solutions will come only when the needs and requirements of all participants are recognized and costs are appropriately shared.

2009
Visiting Scholars

As part of its goal of supporting and adding to the research literature on issues related to consumer payments and consumer credit, the Payment Cards Center created a visiting scholar program in 2001. This program is a collaborative effort with the Bank's Research Department and aims to establish supportive relationships with academic researchers whose interests advance the center's mission. Since 2001, six researchers have participated in the program, working with Research Department economists and center staff, participating in center activities, and assisting the center in setting its research agenda.

This year, Professor David Humphrey, Florida State University, Professor Nicholas Souleles, University of Pennsylvania, and Professor Jonathan Zinman, Dartmouth College, will continue their relationships as visiting scholars at the center.

The center is pleased to announce the appointment of two additional scholars: professors Michael E. Staten and John P. Caskey.

Staten holds the Take Charge America endowed chair in the Norton School of Family and Consumer Sciences at the University of Arizona. He is also director of the Take Charge America Institute for Consumer Financial Education and Research.

He is widely known for his 30 years of policy-oriented research on consumer credit and mortgage markets. His work includes studies of the causes and consequences of consumer bankruptcy, the role credit bureaus play in increasing access to credit, the effects of credit counseling on borrower behavior, the effect of financial education on young consumers, and the benefits and costs of disclosure requirements for consumer credit.

Staten served as director of the Credit Research Center at Purdue University (1988-97), and later as distinguished professor and executive director of the relocated Credit Research Center at Georgetown University (1997-2006), and George Washington University (2006-07). He has taught undergraduate and graduate

Michael Staten

students at Purdue University and the University of Delaware.

He serves as a trustee for the American Financial Services Association Education Foundation and is a member of the Advisory Council for the National Foundation for Credit Counseling.

Staten received his Ph.D. from Purdue University in 1980.

John Caskey is a professor of economics at Swarthmore College. He is widely known for his research on the provision of financial services among the poor and the design and performance of community development financial institutions. His work includes studies of the unbanked population, check-cashing outlets, pawnshops, and payday lenders. He has also written articles on the evolution of the Philadelphia Stock Exchange and the role of network externalities in explaining the gradual adoption of debit cards and the unwillingness of consumers to use the dollar coin.

Caskey taught at Washington University in St. Louis from 1983 to 1988 and was an economist at the International Monetary Fund in 1986. He has been a visiting scholar at the Federal Reserve Banks of Philadelphia and Kansas City, Yale University, and the Universidade Nova de Lisboa. He has served as consultant to the Filene Research Institute, the Ford Foundation, the Pew Charitable Trusts, and the World Bank.

Caskey received a Ph.D. in economics from Stanford in 1984 and a B.A. in philosophy from Harvard University in 1978.

John Caskey

Recent Publications

The Payment Cards Center's commitment to industry analysis and research is fulfilled through its support of consumer payments- and payment cards-related papers written by center staff, visiting scholars, researchers affiliated with the center, and economists in the Bank's Research Department. These papers can take several forms: discussion papers, conference summaries, working papers, or *Business Review* articles. Discussion papers and conference summaries are generally written by center staff and are aimed at industry and policy-oriented audiences. Working papers are intended for the professional researcher and are written by center visiting scholars and economists in the Bank's Research Department. The *Business Review* includes less technical articles written by economists in the Bank's Research Department. Recently published papers are available in PDF format on the center's website. A chronological listing of papers posted to the website in 2008 follows.

2008

Discussion Papers

08-08 New Prospects for Payment Card Application in Health Care

08-09 Legislative Responses to Data Breaches and Information Security Failures

Conference Summaries

09-01 Maintaining a Safe Environment for Payment Cards: Examining Evolving Threats Posed by Fraud

Working Papers

08-18 In Harm's Way? Payday Loan Access and Military Personnel Performance

08-32 Restricting Consumer Credit Access: Household Survey Evidence on Effects Around the Oregon Rate Cap

Business Review Articles

08-05 Ten Years After: What Are the Effects of Business Method Patents in Financial Services?

PAYMENT CARDS
Center

FEDERAL RESERVE BANK OF PHILADELPHIA

Update

Payment Cards Center Newsletter

Federal Reserve Bank of Philadelphia
Ten Independence Mall
Philadelphia, PA 19106-1574
215-574-7220
215-574-7101 (fax)
www.philadelphiafed.org/payment-cards-center/

Peter Burns
*Vice President and Director,
Payment Cards Center*

Christine Lemmon
*Senior Research Assistant and
Update Editor*

The Payment Cards Center was established to serve as a source of knowledge and expertise on consumer credit and payments; this includes the study of credit cards, debit cards, prepaid cards, smart cards, and similar payment vehicles. Consumers' and businesses' evolving use of electronic payments to effect transactions in the economy has potential implications for the structure of the financial system, for the way that monetary policy affects the economy, and for the efficiency of the payments system.