Published by the Payment Cards Center, providing meaningful insights into developments in the payment card industry.

Financial Privacy: Perspectives from the Payment Cards Industry*

A Symposium Sponsored by the Payment Cards Center

Mark Furletti
Stephen Smith

May 2003

Summary: *On Friday, March 21, 2003, the Payment Cards Center of the Federal Reserve Bank of Philadelphia hosted a one-day symposium entitled "Financial Privacy: Perspectives from the Payment Cards Industry." The Center invited legal scholars, federal banking regulators, and privacy officers from the largest credit card issuers and information providers in the U.S. to discuss the key privacy issues facing the industry. This paper provides highlights from the symposium presentations and ensuing discussions.*

* The views expressed here are not necessarily those of this Reserve Bank or of the Federal Reserve System.

FEDERAL RESERVE BANK OF PHILADELPHIA
Ten Independence Mall, Philadelphia, PA 19106-1574• (215) 574-7220• www.phil.frb.org

Introduction

On March 21, 2003, the Payment Cards Center of the Federal Reserve Bank of Philadelphia hosted a one-day symposium entitled "Financial Privacy: Perspectives from the Payment Cards Industry." The Center invited legal scholars, federal banking regulators, and privacy officers from the largest credit card issuers and information providers in the U.S. to discuss the key privacy issues facing the industry.[1] L. Richard Fischer and Oliver Ireland, two privacy experts from the law firm of Morrison & Foerster, were instrumental to the success of the symposium.

The symposium was structured as a roundtable discussion. Participants freely interacted with the discussants and moderators, generating a lively dialogue. What follows are highlights from this event organized around four sessions, including two talks from leading privacy experts and two panel discussions on the information used by card issuers and issuers' information management and compliance practices.

The president of the Federal Reserve Bank of Philadelphia, Anthony M. Santomero, opened the symposium by describing its goals. He expressed the hope that the symposium would provide an opportunity for industry representatives to help inform the debate over financial privacy and assist policymakers in focusing their attention on the key issues. Although regulation surrounding financial privacy is a relatively new phenomenon in the financial services industry, it is clearly of great importance. Given the emerging debate in Congress over financial privacy this term and the significant impact of several lawmakers' proposals, it is important for people on all sides of the debate to consider carefully the industry's privacy practices and the role information management plays in providing efficient and equitable access to credit.

[1] Specifically, the symposium benefited from the perspectives of privacy officers from nine of the largest credit card issuers in the U.S., representatives from the card industry's leading information providers, attorneys from firms that specialize in credit card bank regulation and litigation, law professors, and regulators and researchers from the Board of Governors, Office of the Comptroller of the Currency, and the Federal Reserve Bank of Philadelphia.

Santomero suggested that the meeting's participants focus discussions less on specific regulations and more on developing a fundamental understanding of how card issuers use customer information to improve service levels and what is currently done to protect customer information and comply with applicable regulations. He concluded his remarks by posing to symposium participants the following questions for discussion: What kinds of uses and abuses of consumer information give rise to legitimate privacy concerns? How do current industry practices manage these concerns? How should market forces and prescriptive rulemaking work together to create an environment that is both responsive to consumer needs and protective of consumer interests?

The Financial Privacy Debate

After Santomero's introduction, Oliver Ireland of Morrison & Foerster LLP provided a brief legal history of privacy as a matter of recent public concern. Everyone, he noted, attaches value to privacy; accordingly, it is indisputably a fundamental issue. In the 1960s and 1970s, most of the privacy-related debate in this country centered on government access to citizens' private information, including controlling its use and ensuring its accuracy. Given both the widespread distrust of government that was a legacy of the Vietnam War and the development of mainframe computers, which made the accumulation and storage of detailed information regarding millions of individuals technically feasible, Congress passed several pieces of privacy-related legislation in the 1970s. The Privacy Act of 1974, which applied to records held by the government, and the Right to Financial Privacy Act of 1978, which applied to records held by the private sector, restricted the government's ability to collect and use personal financial and non-financial data. In response to consumers' concerns about the electronic collection and maintenance of personal credit data by "credit bureaus," Congress passed the Fair Credit Reporting Act (FCRA) in 1970. This act set standards for accuracy of and access to credit data.

Though largely dormant through much of the 1980s, the issue of privacy again became a matter of intense public concern with the proliferation of personal computers and the growth of the Internet in the 1990s. In 1996, the enactment of the Health Insurance Portability and Accountability Act (HIPAA) addressed the privacy issue in the context of the doctor-patient relationship. In that same year, the FCRA was amended to include additional privacy protections, e.g., allowing consumers to remove their names from prescreened marketing lists generated from credit reports. In 1999, Gramm-Leach-Bliley (GLB) specifically addressed the use of information by financial services firms. Ireland, who helped craft some of GLB's rules in his former job as associate general counsel of the Board of Governors, described how enactment of GLB raised concern about the sharing of information between industries now permitted to be organized under a unified corporate entity. However, GLB actually focused on the disclosure of information by a financial institution to non-affiliated third parties.[2]

The debate over information-sharing practices and GLB has continued as state and local governments have entered the fray. In addition, privacy issues surrounding telemarketing practices and identity theft have gained in popularity among state and federal lawmakers.

In sum, the political and legislative debates currently surrounding privacy are, in Ireland's view, largely a "hodgepodge." With respect to privacy, it may appear that we do not actually know what it is we are trying to protect. Is it the accuracy of information, control of information about us, or something else? The recent well-publicized incidences of identity theft may have further confused many Americans, who are unsure about how their privacy is threatened and how best to deal with the danger.

---

[2] Professor Peter Swire, one of the symposium's speakers, details the events leading up to GLB and its impact on the industry in a *Minnesota Law Review* article entitled "The Surprising Virtues of the New Financial Privacy Law." A copy of this paper can be found on his web site at www.peterswire.net.
In addition, law professor Anita Allen of the University of Pennsylvania addressed the events leading up to GLB at a Payment Cards Center workshop. A summary of that workshop, entitled "Privacy Matters," can be found on the Payment Cards Center's web page at www.phil.frb.org/pcc/discussion/index.html.

In his concluding remarks, Ireland introduced the further consideration that remedies to deal with privacy protection must be balanced with considerations of cost and the impact on economic efficiency. It is this type of analysis, he suggests, that will help address Santomero's earlier question about the respective roles of prescriptive regulation and market forces in providing appropriate protections.

Perspectives on Privacy: The Banker and the Economist

The remarks by Peter Swire, law professor at the Moritz College of Law of the Ohio State University and former chief counselor for privacy in the Office of Management and Budget under President Clinton, essentially attempted to refute an argument made routinely by many economists: Efforts to protect privacy in the financial services industry (and elsewhere) are obstacles to the functioning of optimally efficient markets.[3] Perfect competition flourishes only where there is perfect information. Privacy rules foster inefficiency by making it more difficult for willing buyers and sellers to connect. Further, by encouraging the strategic withholding of pertinent information, privacy rules prevent efficient transactions from taking place. Such rules may also facilitate the commission of fraud. But this disparaging assessment of the effort to protect privacy, Swire maintains, is fundamentally flawed: Confidentiality often enhances efficiency in the market, and, correlatively, the risk that certain confidential personal information may be disclosed without the information owner's consent (or even knowledge) can easily lead to a significant misallocation of resources. It is also important to note, he argues, that the protection of privacy is a widely treasured value of most citizens in a free society.

The financial services industry has a long tradition of safeguarding confidential personal information. It is inconceivable that such respect for confidentiality in the banking industry could have endured for so long were it, in fact, a detriment to market efficiency. It is obvious, Swire

contends, that certain confidential information, such as the combination to a safe or a computer password, must be kept secret and that doing so does not harm economic efficiency; indeed, the unauthorized disclosure of such information can lead to serious, possibly catastrophic harm. Moreover, our legal system protects trade secrets and certain other confidential business information from unauthorized disclosure in the belief that doing so provides an incentive to businesses to invest in and develop competitively useful information and products. Additionally, examples can be cited where the possibility of the disclosure of certain personal information can prompt individuals to undertake considerable efforts to conceal that information and thereby chill useful transactions even before they occur.

By their behavior, most people, Swire believes, manifest a marked "taste" for privacy, which they regard as a pivotal "right" in contrast to which a single-minded concern for economic efficiency may appear foolish. Most individuals would not view with equanimity the public disclosure of detailed information about their personal lives, including information as seemingly mundane as their purchasing activity. Many Americans report that they worry about a gradual erosion of privacy in the coming decades that may ultimately result in a qualitatively less desirable society. There is also evidence to suggest that in cases where they are confident a bank has justifiably earned a solid reputation for adequately protecting confidential personal information, consumers will voluntarily engage in additional activities involving that institution, including online banking.

In sum, the standard efficiency analysis of rules protecting privacy advanced by some economists ignores multiple concerns made evident by other approaches. Moreover, it is unquestionable that, in many settings, confidentiality promotes efficiency. Even where efficiency may be harmed by privacy, there are certainly situations in which many individuals would reasonably conclude that the protection of their privacy is the greater good and worth the cost.

---

[3] Professor Swire's talk was based on a paper he released at the end of last year entitled, "Efficient Confidentiality for Privacy, Security, and Confidential Business Information." A draft of this paper can be

Information Used by the Card Industry

The first panel of the day brought together L. Richard Fischer of Morrison & Foerster as moderator and Robert Ryan of TransUnion, along with Timothy Spainhour of Acxiom, to discuss the different kinds of information on which credit card issuers rely. TransUnion, one of the country's three leading credit reporting companies, and Acxiom, one of the largest repositories of non-credit consumer data, provide credit card issuers with the information used to assess a consumer's creditworthiness and likelihood of responding to a given offer of credit.

After providing brief histories of their respective companies, Ryan and Spainhour explained how the data their companies provide to credit card issuers increase the efficiency of the credit granting and solicitation process. In Ryan's view, the data collected and disseminated by TransUnion and the other major credit reporting companies have significantly contributed to broader levels of credit access and more rapid credit decisions. Overall, the existence of an easy-to-access and up-to-date national credit tracking system significantly lowers the cost of consumer credit. Without such a system, prospective borrowers would likely have to fill out lengthy and intrusive applications, and lenders would have to take much more time to review and verify consumer-supplied financial data.[4]

Ryan also explained how credit bureau data have drastically altered the way consumers shop for credit. Instead of consumers' having to seek out lenders when a borrowing need arises, lenders seek out creditworthy consumers by "prescreening" credit files. Prescreening allows issuers to pass credit criteria to a credit reporting company and make firm offers of credit to those who meet the criteria. It is estimated that accepted prescreened offers account for 50 to 90 percent of most major issuers' credit card accounts. For many consumers, this essentially means that shopping for credit involves little more than a trip to the mailbox.

---

found on his web site at www.peterswire.net.

[4] For more information about credit reporting, please refer to the following two Payment Cards Center discussion papers: "An Overview and History of Credit Reporting" and "What's in the File? The Economics

Ryan concluded by discussing the consumer protections provided by the Fair Credit Reporting Act (FCRA). The act sets forth rules for handling consumer disputes, restricts the amount of time that adverse information can remain in a consumer's file, allows consumers to remove their names from prescreened lists, and strictly limits the purposes for which an entity may gain access to the reports. These provisions, Ryan asserted, effectively balance consumers' interests in data accuracy and confidentiality. The law also prohibits states and municipalities from enacting laws that conflict with certain provisions of the FCRA, including those that pertain to prescreening. These pre-emptions, however, will expire on January 1, 2004 unless Congress acts to extend them. Ryan, along with many other symposium participants, strongly advocated a permanent extension of the federal pre-emptions. If federal pre-emption is allowed to sunset next year and credit bureaus are forced to comply with different state- and/or municipality-created rules, Ryan predicts that credit bureau data could lose much of their completeness and richness.[5]

In contrast to credit bureau data that are used to determine who qualifies for credit, the consumer information maintained by Acxiom allows issuers to determine which creditworthy consumers might be interested in a particular product. This kind of consumer information reduces issuers' direct mail and telemarketing expenses, helping them avoid the solicitation of unreceptive consumers. Essentially, non-credit consumer information is a tool issuers use strategically to target credit offers and maximize the value of mail, telephone, and Internet marketing efforts.

Spainhour emphasized that Acxiom does not provide its clients with consumer "dossiers." Instead, Acxiom helps companies focus their marketing efforts by providing them with the names and addresses of people who meet certain marketing or response criteria. In fact, he argued, the company's sophisticated database technology provides its own privacy protections by eliminating

---

and Law of Consumer Credit Bureaus." Both can be found on the Center's web site at www.phil.frb.org/pcc/discussion/index.html.

[5] The AEI-Brookings Joint Center for Regulatory Studies released a paper in March 2003 that examines the FCRA preemption issue in great detail. The paper, "Financial Privacy, Consumer Prosperity, and the Public Good: Maintaining the Balance," can be found on the web page of one of its authors, Professor Fred Cate, at www.law.indiana.edu/directory/fcate.asp.

the need for human intervention in the assessment of information gathered on individuals and their purchasing behavior. Consumers who do not wish to be included on Acxiom's lists have the opportunity to opt out by contacting Acxiom directly, contacting the Direct Marketing Association, or placing their names on state "do not call" lists. Acxiom also works to ensure that its clients are not misusing consumer information. It frequently "seeds" the lists that it sends to clients with the addresses of Acxiom compliance officers in order to monitor offers generated from Acxiom data.

Spainhour suggested that the privacy debate, to a large extent, is about control. If consumers feel they have no control over how their personal information is used, they will likely be suspicious of companies that collect consumer information and may work to make data collection more difficult (e.g., by using aliases or fictitious identities). Conversely, to the extent that consumers know they have control over their personal information and have confidence in its not being misused, they will be less concerned that their privacy is being compromised. One of the most important things that the industry can do, Spainhour suggested, is to make consumers aware of the controls they have over their personal information.

Many symposium participants agreed with Spainhour's assessment. They further argued that to the extent companies like Acxiom have a good understanding of an individual's preferences, marketers can do a better job of soliciting that individual. For example, if a firm was about to launch a telemarketing campaign and it had a list of people who had never bought a single product over the telephone, marketers would likely choose not to call the people on that list. In this way, pieces of personal information can help companies spend marketing dollars more wisely and minimize the solicitations consumers receive.

The Card Industry's Information Management and Compliance Practices

Andy Navarrete, associate general council for policy affairs at Capital One; Bill Brooks, chief privacy officer at MBNA America; and moderator L. Richard Fischer led the second panel

discussion on how credit card issuers use and protect consumer data. MBNA and Capital One are among the largest consumer lenders in the US, both specializing in credit card lending.

Brooks and Navarrete explained how their organizations have changed in response to Gramm-Leach-Bliley. In addition to investing in systems to track privacy policies and coordinate privacy mailings, both issuers have created senior management positions and dedicated committees that are specifically charged with examining privacy and data security issues. At MBNA, Brooks reviews every third-party request for customer data; no data are sent outside of the bank without his express permission. Capital One has centralized privacy management and frequently convenes meetings with senior managers to examine each area's adherence to the issuer's privacy policies.

Overall, both issuers agreed that the enactment of GLB's privacy provisions had beneficial effects on the industry. Fischer, as moderator, expanded on these comments. He believes that GLB has led to stronger data security procedures, better documented and better understood information flows, and much improved privacy management as it relates to issuers' third-party relationships. Participants generally agreed that their banks' investments in implementing GLB's provisions either had paid off or would soon pay off. One bank's privacy officer, however, argued that while there have undoubtedly been benefits in some areas, he saw little good coming from the annual notice provision of GLB. He noted that compared with the money spent on developing and implementing a privacy policy, the annual notice mailings involve disproportionately high printing and mailing costs and do little to effectively inform consumers. Participants uniformly agreed that the privacy notices required by GLB do not work and should be modified. Many advocated a "stepped" model. That is, all customers would receive a nutrition-label-like notice that highlights key privacy protections, and customers who request it could get a copy of the entire policy.

A number of participants argued that market forces provide consumers with important privacy protections. Navarrete explained how Capital One tries to differentiate itself from its

competitors by using its strict privacy policy to its advantage and offering products with a no telemarketing guarantee. Some banks, Oliver Ireland noted, have made the decision to forgo the revenues associated with cross-selling marketing partners' products and tout this fact when trying to attract potential customers. He also explained that banks that fail to appropriately protect their customers' data or compromise their customers' privacy can face harsh consequences from regulators and consumers. The cost of getting privacy wrong, Ireland said, could be the loss of an issuer's business.

Many participants also agreed that the current opt-out regime that governs affiliate sharing is far preferable to an opt-in regime. Opt out begins with the assumption that all customers want their information shared with an issuer's marketing partners; only the information of those who express otherwise is not shared. Opt in begins with the assumption that no customers want their information shared. The issuer can share only if it receives express permission from the customer. Under the current regime, less than 5 percent of an issuer's customers typically opt out of affiliate-sharing efforts. While most agreed that opt out was preferable and offers consumers sufficient protection, there was some feeling that opposing views were gaining political momentum. One issuer's privacy officer noted that universal adoption of opt in was something for which his company was preparing.

At the conclusion of his remarks, Navarrete strongly advocated applying customized remedies to privacy issues. "Privacy" is often used as a term of convenience. It means different things to different people. Instead of debating the meanings of privacy and the merits of opt-in and opt-out regimes in this overly broad context, he argued that the industry and policymakers should focus on solutions that target specific problems. He suggested, for example, modifications to rules to make it easier for victims of identity theft to correct their credit reports. He also proposed privacy notice reform to improve transparency. The privacy issues that most concern consumers, he believes, are best addressed on a case-by-case basis.

Conclusion

In 1890, the *Harvard Law Review* published "The Right to Privacy." In that article, Samuel Warren and Louis Brandeis proposed the following:

> Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone."

The devices that offended the public's sense of privacy in the late 19th century were machines that could take "instantaneous photographs" and record voices. People were concerned that their pictures and words could be circulated without their permission. It is interesting in this context to consider the historical impact of technology on the evolution of the privacy debate. It is perhaps not coincidental that the flurry of activity in this area in the 1970s corresponded to the introduction of personal computers and distributed data management capabilities and that the current wave of privacy legislation comes amidst the proliferation of the Internet. While technologies may have changed, the underlying principles surrounding the privacy debate have not. Public policy and market forces continue to balance consumers' "right to be let alone" with card issuers' and other businesses' rights to gather and use consumer data to offer and improve products and services.

One hundred years ago, privacy was an issue involving the use of unauthorized photographs and recordings. Forty years ago, as Oliver Ireland points out, privacy was about protecting people from governmental intrusions. Today, the debate seems to focus on the use of personal financial and medical information by private businesses. It is obvious, then, that the word "privacy" can connote different things at different times. Symposium participants suggested that the word "privacy" can also connote different things to different people.

The multifaceted and somewhat elusive nature of privacy, Ireland suggests, is one of the leading reasons it attracts so much attention from federal, state, and local lawmakers. Although privacy manifests itself as a series of discrete policy issues — e.g., federal pre-emption of the

FCRA, privacy notices, affiliate sharing, joint marketing agreements, data security — the values that privacy legislation purports to protect are somewhat unclear.

It is clear, according to Swire, that confidentiality and security, two issues related to privacy, are important ingredients in a well-functioning economy; they induce parties to trust each other. Thinking about privacy in the context of business relationships, he suggests, may help issuers better understand how and why consumers value it.

Another privacy issue involves the collection and maintenance of personal information. Ryan asserts that there are compelling public policy reasons for maintaining federal information standards. Spainhour suggests examining the issue from the perspective of consumers. Instead of thinking in terms of opt in and opt out, consumers focus on more concrete things, such as phone calls that interrupt dinner, a mailbox full of credit card solicitations, anonymous eyes poring over the details of their private lives, and the specter of identity theft. Education, Sapinhour proposes, is critical. If consumers know that when and if they require it, they have control over their personal information and understand exactly how it is used, they will feel less anxious about their privacy being compromised and perhaps gain a better understanding of the benefits that accrue from the accumulation and controlled disclosure of that information.

For credit card issuers, privacy involves yet another set of issues. Brooks points to the resources credit card companies have invested in keeping customer data secure. Unless an issuer can ensure data's safekeeping, its privacy policies and procedures have little significance. Navarrete suggests that market forces can further address privacy issues. As a focal point of competition, an issuer's privacy policies can be used like any other product feature to attract consumers. For those privacy issues the market cannot solve itself, Navarrete suggests rules that precisely target specific problems (e.g., identity theft). Finally, Fischer points out that the current privacy framework established by GLB has greatly improved the industry's understanding of its own information-sharing practices. Armed with a detailed understanding of how data move inside

and outside of the organization, senior managers have put in place controls that protect consumers from privacy invasions and protect banks from security breaches.

It was clear from the day's discussion that the privacy debate cannot be resolved with a single piece of legislation or a single administrative agency's rule. The issue is simply too broad, its facets too complex, and the technology that gives rise to these concerns too dynamic. Instead, the questions surrounding privacy require careful dissection, extensive analysis, and tailor-made remedies. While symposiums often raise as many questions as they answer, participants in this event agreed that industry leaders and policymakers must focus first on defining the nature of the privacy issue being debated. Such thoughtful consideration may lead to appropriate remedies. That is, for some issues, the response may require attention to data security. For other issues, more aggressive law enforcement or improved transparency may be needed. With an understanding of specific issues, one can then determine whether the perceived danger is best solved through prescriptive rulemaking or whether market forces can be relied upon to provide a solution. In the end, the goal should be to understand clearly the specific privacy interests that need to be protected and to implement safeguards in a way that efficiently balances relevant costs and benefits.

Conference Summary

PAYMENT CARDS CENTER

Financial Privacy:
Perspectives from the Payment Cards Industry

Symposium Speakers and Discussants

- **James W. Brooks, Jr.**, *MBNA America*
- **Peter Burns**, *Federal Reserve Bank of Philadelphia*
- **L. Richard Fischer**, *Morrison & Foerster, LLP*
- **Oliver Ireland**, *Morrison & Foerster, LLP*
- **Andy Navarrete**, *Capital One*
- **Anthony M. Santomero**, *Federal Reserve Bank of Philadelphia*
- **Robert Ryan**, *TransUnion*
- **Tim Spainhour**, *Acxiom Corporation*
- **Peter P. Swire**, *Moritz College of Law of the Ohio State University*

FEDERAL RESERVE BANK OF PHILADELPHIA
Ten Independence Mall, Philadelphia, PA 19106-1574• (215) 574-7220• www.phil.frb.org