Sensitive Information in Financial Services

CS 457a

Gus Fuldner

Introduction

Financial services is fundamentally an information-driven industry. Consumer financial transactions generate huge amounts of personal data. Every ATM transaction, credit card purchase, check deposit, and loan application leaves electronic traces in the form of transaction records at both your bank and (often) the counterparty's financial institution. The sheer volume of such transactions is huge, Visa's USA division alone processed 14 Billion transactions in 2002.[1] Financial institutions can use the information acquired in the course of business beyond the basic function of rendering the service requested by the consumer. Databases of customer data and provide insights in to customer habits and allow institutions to connect consumers with products they are likely to want. Detailed transaction databases also allow financial institutions to more efficiently price products. For example data mining tools enable better estimate and understand important costs that are not known *a priori* such as credit risk and price loan products accordingly.

There is little question that customer information is quite valuable to businesses. For years, the courts have held that customer list are valuable and can be protected as trade secrets. Financial information is an interesting class of personal information to look at from a privacy perspective because it exists in large quantities, is non-public, and is often sensitive, yet a singly piece of information can be handled by a wide range of entities. Clearly, some level of information sharing is needed to effectuate financial transactions. It would not be possible, for example, to deposit a paycheck in your bank with out your employer and its bank also knowing the important details. While a consumer understands this necessity, advances in databases and communication technology now allow financial institutions to compile vast amounts of data about their customers and even create profiles of their personal financial habits.

---

[1] http://usa.visa.com/personal/newsroom/1trillion.html

There are two primary areas of concern about privacy and sensitive data handling in financial services: information sharing, and information security. These two classes of concerns are often mixed together, but should be thought of as largely distinct issues. Information sharing concerns the *intentional* use and distribution of personal information. Many consumers are uneasy about the amount of information that their financial institutions know about their lives and what firms may be doing with that information. Information security questions center around *unauthorized* use of personal information. The principal concern is the risk of some sort of identity theft, but may also include unauthorized disclosure of sensitive personal information such as your wealth or spending habits. Information sharing and information security issues both concern the distribution of non-public personal financial information, but they each require fundamentally different approaches, both procedurally and technically, to addressing the needs of consumers.

Information Sharing

The tremendous advances in information technology have led some to question when financial institutions should be able to share information about its customers with other businesses. Consumer advocacy groups want to restrict information sharing and have lobbied for "opt-in" laws that would require institution to obtain explicit consent prior to sharing personal information to third parties. Such a system would likely force financial institutions to compensate customers with incentives such as lower fees, better interest rates, etc. in order to induce customers to authorize sharing of their information. Obviously these inducements would be limited to something less than the value that the institution can generate from this right to share information. While not driven by a legal requirement, this is essentially the way that grocery store discount cards work. Grocery stores provide cardholders with special discounts in exchange for the ability to track a customer's buying behavior by studying card usage. While many consumers may think

more about the potential savings than the loss in privacy, the grocery card has essentially created a market system for acquiring privacy rights from its customers.

The Graham Leach Bliley Act of 1999 (GLB) does not go so far as requiring opt-in consent for information sharing, but it does financial institutions to allow consumer's to "opt-out" of the firms right to share the customer's information to non-affiliated third parties. Beginning July 1st 2001, financial institutions that share information with any non-affiliated third parties had to provide written privacy policies that describe what information is collected by the institution and precisely what may be shared with third parties. Institutions must provide this notice annually and consumers must be given an opportunity to opt-out of unwanted information sharing.

The opt-out approach is clearly favors financial institutions because they are allowed to share information by default. Jeffrey Lacker, a Fed economist, argues that from an economic perspective the distinction between opt-out and opt-in should be no different than the difference between treating CD players as standard equipment or an available option in a new car.[1] Because institutions can still provide incentives to induce its customer's not to opt-out, the overall compensation provided to consumers for the right to share their personal information should be the same. One would expect, however, that a larger proportion of customers would not opt-out from information sharing than would opt-in under and opt-in scheme. While consumer advocates may criticize GLB for having an opt-out system, any difference in information sharing authorized under one scheme or the other reflects indifference about information sharing among a portion of the population. Why not allow financial institutions to share their information if they don't seem to care that much? While exact figures are not available, industry sources cite an opt-out rate of about 5% for GLB-related privacy notices.[2]

The information sharing debate is fundamentally about the ownership of information rights. The opt-out rules and privacy policy requirements of GLB provide a clear mechanism for assigning information distribution rights between the institution and the customer. It is up to the markets to determine the value of these information rights. Institutions can provide incentives to customers who do not opt-out of its information sharing policy. Similarly, institutions can and do compete on privacy policy issues. Capital One's No-Hassle Card and Citibank's Illumina claim no telemarketing calls, and no sharing of personal information to third parties. The actual benefits offered by both cards does not substantially exceed what a diligent consumer could accomplish with opt-out choices and do-not-call lists.[3] The popularity of these cards seems to suggest that consumers care about privacy, but do not fully understand their basic privacy rights.

Given that GLB provides market-base system of assigning privacy rights, the other remaining issue is how should financial institutions ensure compliance with a consumer's preferences. This issue can be divided into to parts, preference recording, policy management. Preference recording is the need to record each consumer's opt-out choice. This problem is really a matter of recording a single yes/no bit with each customer record, a simple database task. Policy management is a more complicated matter that involves how to ensure that the firms actions comply with the its stated policy.

Institutions are required to designate an Information Security Officer who is specifically responsible for overseeing information security and sharing within the firm. GLB provides many exceptions to the opt-out requirements for information disclosure. The exceptions allow the institution to disclose non-public personal information about its customers to non-affiliated third parties to perform various functions such as transaction

processing, loan servicing, fraud prevention, or for the purpose of considering a sale of accounts or of the financial institution itself. These exceptions are designed to allow financial institutions to outsource back office tasks and to prevent unreasonable compliance requirements in certain situations.

An important part of a privacy policy management program is training and education within an institution about what information sharing falls under the statutory exceptions and what requires observation of opt-out preferences. Training and education to make employees conscious of privacy principles is as important as any technical barriers to information sharing as even well-meaning employees can unknowingly violate a company's privacy policy.[2]

To prevent secondary disclosure of non-public information, non-affiliated third party recipients of customer information that fall under the exception to the opt-out requirements must be covered by confidentiality agreements to prevent disclosure to additional non-affiliated third parties. Data handing and confidentiality agreements are an important part of the information technology portion of an institutions regulatory review. The Federal Financial Institutions Examination Council (FFIEC), a consortium of the major bank regulatory agencies, has extensive guidelines with specific requirements and recommendations for financial institutions to follow when contracting for and managing outsourcers that are discussed further in the Information Security Section of this paper.

---

[2] For example, JetBlue shared passenger information with a government contractor working on a national security-related data mining project in violation of its own privacy policy.

While GLB defines industry-wide requirements limiting information sharing, there are few industry-wide standards that communicate privacy policy information. Financial institutions have generally adopted a binary approach to the opt-out requirements. I could not find any institutions with a rich set of differing privacy options. Given these binary choices, there is little need for a complex privacy preference communication standard such as P3P. The only standard for communicating privacy preferences is an extension to the emerging IFX (Ineractive Financial eXchange) standard for XML-based communication between electronic bill payment and presentment systems (EBPP) that presents disclosures and provides a standard way of recording their acceptance and associating that information with customer transactions.[3] IFX is still an emerging communication standard and it is unclear if this feature is actually used anywhere in practice, but is nonetheless a step in the direction of standardized IT privacy management protocols. EBPP is a good candidate for privacy protocols because it involves many-to-many communication among consumers, bill pay services, and billers.

Perhaps it should not be surprising that there aren't major industry standards for describing data privacy requirements. Most sharing of information that a financial institution might do would require contractual negotiations, which would likely cover confidentiality of customer information, and technical negation on issues such as data formatting, which could likely include any privacy information that may need to be communicated between IT systems. More generally, the issues that financial institutions face in information sharing have more to do with corporate policy decisions than specific technical processes.

---

[3] www.ifxforum.org

Information Security

The basic information security needs of financial institutions are very similar to those of most large corporations. The problem is that financial institutions are generally fairly high value targets. Gaining unauthorized access to a financial institution's customer records can make identity theft easy on a large scale. Unauthorized access to customer information creates operational, legal, and reputational risks for financial institutions. Each of these risks are part of the standard risk dimensions measured by financial regulators such as the Federal Reserve Board when evaluating the soundness of financial institutions.[4] Clearly there can be real costs related to information security lapses in the form of increased fraud, false transactions, legal liability, and loss of customers. The regulatory agencies are most concerned about the soundness of the institutions that they oversee so the regulations tend to focus on issues that would be most likely to result in a significant financial loss to the institution.

The FFIEC publishes an Information Technology Examination Handbook that describes information security best practices in extensive detail including, access control, physical security, encryption, system and network design, personnel, logging, service provider oversight, intrusion detection, and business continuity planning. The recommendations range in technicality from the basics of passwords to how to organize DNS and NAT to segregate internal corporate networks. The IT Examination Handbook has extensive guidelines covering oversight of third-party service providers including

[4] Other risks include credit and market risk. Other regulators include the Office of the Comptroller of the Currency, the Office of Thrift Supervision, the National Credit Union Administration, and Federal Deposit Insurance Corporation

formal audit procedures and coordination of security reviews for service providers that service multiple institutions.[4, 5] All of the IT examination materials have been updated recently to reflect the increased scrutiny of IT systems in financial institutions that is required under the Safeguards rule of GLB. This represents a significant step forward in technology oversight of financial institutions that hopefully will pay off in the future in terms of fewer information security failures at large banks. The trend towards large financial conglomerates and their associated large, distributed technology environments will continue to be a challenge to managing information security in large institutions.

The GLB guidelines and the majority of the examination rules focus on unauthorized access to data from external sources. One of the largest problems with controlling information in large financial institutions is how broadly accessible information is across an enterprise. For example, bank tellers often have access to very large amounts of data even though most of it may not be necessary for their work. Similarly, software developers often have unrestricted access to customer information, which is justified within the firm as necessary for testing or development. Wide data access makes employees, well-meaning or malicious, a large hole in the information security system. Clearly employees need access to information, but compartmentalizing information so that employees have regular access to only what they need can go a long way towards diminishing risk of personnel-related information security lapses. Perhaps more than any other industry, the majority of bank core processing systems are still based on legacy mainframe systems that were not designed with privacy or complex access control in mind.

As institutions begin the difficult task of replacing these systems over the coming years, it is important to include advanced internal access control and auditing features. The technical needs for such system are similar to many current initiatives in trusted computing. Institutions need verifiable internal data handling systems that can segregate and compartmentalize its customer's personal information by sealing it cryptographically and restricting access to approved situation. A privacy-aware bank IT system might limit a teller's access to customer information to the particular customer he or she is serving by verifying the customer's bank card or other identification before providing data access to the teller. Exceptions to the teller's access could be approved by a manager and logged for auditing purposes. Software development could be done with unprotected test information. Access to real customer data would be restricted to communication by and between privacy-aware applications. The most important feature of a privacy-aware IT infrastructure would be a structured and auditable access control system that limits access to clear text data to those that need to know. If employees know that data handling exceptions are recorded the chance of internal data theft would be greatly diminished. Additionally, requiring manager approval or a similar dual-control system for deviations from the data access standards forces employees be cognizant of information security issues. Unfortunately, given that most bank core processing systems are based on fragile legacy mainframe systems that are difficult to modify it seems unlikely that sweeping changes in data handing practices will occur in all but the most progressive institutions anytime soon.[5]

---

[5] See "IBM pushes new bank apps" *Computerworld*. 11/24/03 for a description of the current state of bank core processing systems and the costs associated with replacing them.

Another potential area for improvement in information security within the financial services industry is in the transaction processing infrastructure. While electronic financial transactions have been growing in popularity for decades, the systems that connect financial institutions to process transaction over credit card, ATM card and ACH networks are surprisingly primitive. While communications communication between various parts of the network is encrypted or travels over private networks, the actual means of authenticating financial transactions is quite primitive. Only the PIN-based ATM card networks have any sort of cryptographic protocol for authenticating transactions. The bank that issued the card approves credit card transactions electronically, but the cardholder's identity verification still relies merely on his or her signature.[6] A customer's name and card number travel through a long chain of middlmen from the merchant back all the way to the issuing bank in the process of authorizing and settling a credit card transaction. Modern cryptographic techniques are at the point where it is possible to create auditable transaction processing systems that do not need to pass significant consumer personal through the processing network. The ACH network for electronic check transactions is even more primitive. There is essentially no built in authorization system at all. Access control is done entirely by the institution that is initiating the transaction and is based on its trust in the customer it is dealing with. For example, Paypal uses a system where you must verify every account at another institution you want to transact with by testing if the customer has access to the account statement information by making two small transactions and asking for the amounts of those

[6] Or in the case of online purchases the purchaser's inentified by the address verification system (AVS), which relies on the purchaser's knowledge of the billing address to authorize the transaction.

transactions. One an account is verified there are transaction limits that limit Paypal's financial risk in the event that the transactions are not actually authorized. Overtime it appears that the industry will slowly move towards more cryptographically secure authorization systems. It would seem logical at first glance that the financial networks that drive global commerce would have stringent cryptographic transaction authentication systems, but in reality these systems are not particularly sophisticated and work because institutions can manage the risk of unauthorized transactions through other means. There is some indication of a movement towards more robust authorization systems PIN-based ATM networks are growing in popularity as banks and merchants realized that the lower fraud risk that results from the strong authorization system means lower overall transaction costs. Financial institutions are making an economic decision that weighs the cost of moving to a new, more robust, transaction processing system with the benefits of better risk management.

Conclusion

The financial services industry has major challenges in dealing with sensitive personal information. This paper has argued that information sharing in financial services is fundamentally a business and economic question of the assignment of information rights between a consumer and a financial institution. While consumer advocates may propose various technical or legal solutions to what they see as a problem of increased information sharing and invasion of privacy, it is fundamentally an economic question that, given an appropriate regulatory framework such as GLB, should be borne out through competition between institutions on the basis of privacy and/or the

value given to those who don't mind giving it up. Information security also turns out to be a largely economic issue in financial services. Bank regulators are largely interested in information security because of the potential financial losses related to security lapses. One could argue that financial institutions do not sufficiently bear the financial cost of information security failures and that it is the customer whose data was revealed or identity stolen who bears the cost. The safeguards rule of GLB begins to address that problem by making information security protections a statutory requirement. Monetary penalties for information security failures would be one way to induce financial institutions to make larger investments in information security and privacy. If consumers demonstrated that the were willing to pay for privacy it is likely that more institutions would make an effort to compete on privacy and information security and implement next generation privacy management technologies.

Bibliography

1. Lacker, Jeffrey M., *The Economics of Financial Privacy: To Opt Out or Opt In?* The Federal Reserve Bank of Richmond Economic Quarterly, 2002. **88**(3): p. 1-16.
2. Lee, W.A., *Opt-Out Notices Give No One a Thrill*, in *American Banker*. 2001. p. 1.
3. Lee, W.A., *Critics: Privacy Cards Market to Ignorance*, in *American Banker*. 2002. p. 12.
4. *Information Security Booklet*, in *IT Examination Handbook*, FFEIC, Editor. 2002. p. 118.
5. *Supervision of Technical Service Providers*, in *IT Examination Handbook*, FFEIC, Editor. 2003. p. 68.