payments system research briefing

OCTOBER 2009 | FEDERAL RESERVE BANK of KANSAS CITY

The Benefits of Collecting and Reporting Payment Fraud Statistics for the United States

by Richard J. Sullivan, Senior Economist

Fraud using various payment instruments—such as checks, debit cards, and credit cards—is a problem worldwide. Payment fraud occurs when someone gains financial or material advantage by using a payment instrument (or information from a payment instrument) to complete a transaction that is not authorized by the legitimate account holder. A lack of statistics for the United States, however, makes it difficult to get a sense of the dimension of the problem.

This *Briefing* first discusses the need for collecting and reporting payment fraud statistics for the United States. It then reports several examples of useful information on payment fraud for Australia, France, Spain, and the United Kingdom. The *Briefing* concludes by exploring the potential costs of compiling more complete payment fraud statistics for the United States.

Why the lack of payment fraud statistics is a problem

Inadequate statistical information on payment fraud in the United States has several consequences. It can mask insufficient resources being devoted to combating payment fraud. Even with adequate overall resources, it can lead to inefficiency if some of those resources are targeting unimportant causes. And it can prevent effective coordination efforts that improve payment security among all payment participants. The lack of good statistics can be seriously misleading, causing us to miscalculate our progress in combating fraud and fail to notice liability shifts. Ultimately, the lack of payment fraud information could lead consumers to unnecessarily lose trust in payments.

The efficiency of efforts to prevent payment fraud depends on access to relevant measures of the risk of fraud. The vulnerability to fraud of Internet purchases, ATM withdrawals, or other transactions is uneven. Without good measures of fraud rate in each of these circumstances, we cannot properly target methods that can prevent payment fraud in more risky situations. Similarly, payment authorization methods vary in effectiveness at preventing fraud in different countries and in different types of transactions. This can lead to differences, for example, in the likelihood of fraud for domestic and international transactions.

Statistics on fraud losses for all of the participants in the payment system would also help to coordinate fraud control. Because payments rely on network technology, there is considerable interdependence and associated spillover effects. A security failure in one element of the payment network can adversely affect others.[1] Similarly, if one element of the payment network improves its security, others can benefit.[2] Consequently, coordination of security efforts is beneficial.

Partial information on payment fraud can be useful but may not necessarily be representative. A commonly cited statistic on fraud loss rates in the United States is for card issuers that are part of the large credit card companies (Visa and MasterCard). Effective strategies to combat fraud have caused a decline in fraud loss rates for this segment of the payment network.[3] While this is good news, we cannot be sure that this is also true for other payment participants. For example, after several years of decline in the number of victims of identity fraud in the United States, a recent survey suggests a considerable rise for 2008.[4]

Focusing on a particular segment of the card network can also hide shifts of losses among payment participants. It is natural for individuals and businesses to work hard to avoid their own fraud losses, but these efforts are going to work best for those with access to effective means of avoiding losses. Corporations, for example, are frequent targets of payment fraud but avoid most losses because they create internal processes to reduce fraud or use fraud control services from their financial institution.[5] Moreover, all payment participants have some incentive to push losses off to other segments of the industry. One concern is that the terms and conditions of computer programs used to process payments are overly protective of software companies. Such terms and conditions may allow a software company to avoid liability in cases of failure that lead to fraud for which it may be responsible.[6] Disaggregated information on payment fraud would help to reveal these types of shifts.

Most important, availability of this type of information lets consumers know that the industry is serious about fraud prevention, which contributes to critical public confidence in the retail payments system. Consumers are sensitive to security failures of the payment instruments they use. In three separate surveys of U.S. consumers from 2003 to 2008, between 45 and 53 percent of respondents expressed "concern" or "extreme concern" over payment fraud and identity theft.[7] Surveys have also shown that awareness of data breaches can change payment behavior among consumers.[8] Regularly reported statistics on payment fraud would provide an anchor to consumer perceptions of payment safety and help prevent inaccurate concerns that may be based on incomplete information.

Fraud losses on card payments in other countries

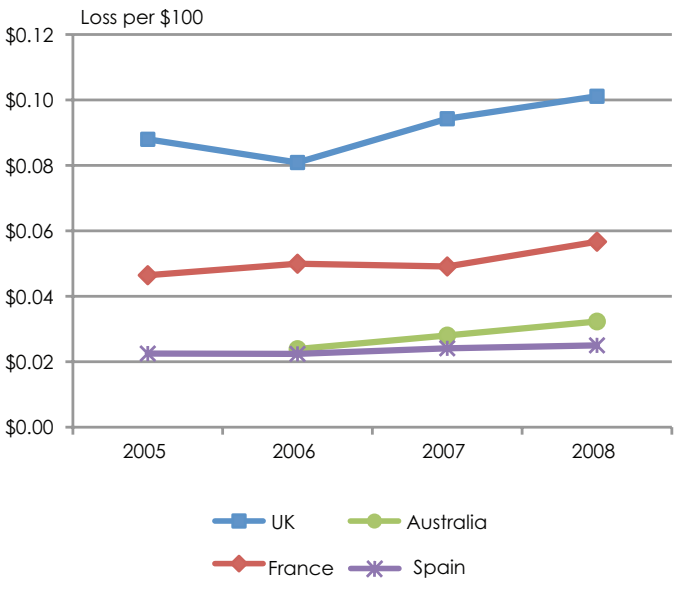
Some other countries are further along than the United States in providing fraud statistics. For example, statistics reported for Australia, France, Spain, and the U.K. show the aggregate levels and trends in payment fraud. For some of these countries, statistics reveal more details, such as higher risk in certain transactions and in various locations.

The statistics are compiled and reported by government or industry-sponsored organizations that gather information.[9] By collecting information from all major industry participants such as card networks, card issuers, and merchants, they avoid the problem of partial and unrepresentative statistics noted in the previous section. These sources typically provide statistics on gross fraud losses (the monetary value of payment fraud before any funds are blocked from transfer or are later recovered) on payment instruments issued by domestic institutions and used in domestic or international transactions.

The accompanying chart shows overall loss rates on payment card (debit and credit) transactions from 2005 to 2008.[10] These statistics show that the U.K. has the highest rate of fraud losses; Australia and Spain have the lowest; and France is in the middle. The extent of the difference is significant: The highest rate of fraud is at least three times that of the lowest. The chart also reveals that the trend in fraud rates is holding steady in France and Spain but rising in Australia and the U.K.

Fraud Losses Per Value of Transactions

Domestically Issued Debit and Credit Cards



Numerous factors contribute to these intercountry differences in fraud rates. These factors would need to be analyzed thoroughly before we could understand how important factors, such as transaction patterns or security standards, account for different fraud rates shown in the chart. While such an analysis is beyond the scope of this *Briefing*, statistics provided by each country provide enough detail to shed light on the sources of fraud and types of transactions that are more susceptible to fraud.[11]

An example of a risky type of transaction, called a card-not-present (CNP) transaction, takes place on the Internet, by mail order, or over the telephone. Payment authorization processes are less able to screen out fraudulent transactions in CNP situations because the merchant cannot inspect the card for counterfeits or confirm that the customer has possession of the card. Merchants in all countries who accept CNP transactions face relatively high fraud rates. In fact, according to the most recent reports, the top source of payment fraud in Australia and in the U.K. is CNP transactions.

CNP transactions are not always the main source of payment fraud because shopping patterns also play a role. A recent European Commission study showed, for example, that only 20 percent of individuals ordered goods over the Internet in Spain, compared to 57 percent for the U.K.[12] Statistics reported for Spain show that card theft is currently the source of most fraud losses, though it is likely that CNP transactions will become a more important source of fraud as Spanish merchants develop their online sales.

Payment security standards are evolving and having an impact on fraud loss rates. An important example is the use of "chip-and-PIN" payment cards, which have an embedded computer chip and require use of a PIN to initiate a transaction. These cards provide more accurate authorization decisions because they more securely authenticate a payment card, and they make it very difficult to counterfeit a payment card. They are currently being adopted in many countries around the world. Statistics reported for the U.K. show that chip-and-PIN has been very successful at reducing fraud on face-to-face transactions, ATM withdrawals, and lost and stolen cards.

Because chip-and-PIN adoption rates differ among countries, the strength of payment authorization processes also differs. As a result, the mix of domestic and international transactions of its cardholders is a factor in a country's fraud rate. Both France and the U.K. have completely transitioned to chip-and-PIN cards. These two countries have reported statistics showing that fraud rates are much higher for international than domestic transactions.

Statistics also reveal that that payment fraud has migrated to locations with weaker card security. Prior to adoption of chip-and-PIN, fraud for U.K.-issued payments cards on transactions outside of the U.K. was about 25 percent of the total but today exceeds 60 percent. Although fraudsters are targeting a wide number of countries, much of this growth has been on transactions in the United States, which does not use chip-and-PIN payment cards.

Collecting and reporting statistics on payment fraud in the United States

Despite the dangers posed by a lack of statistics on payment fraud, the United States does not have a system to collect and report aggregate fraud loss information. Replicating the reporting systems used in other countries would be relatively inexpensive. At a minimum, a similar system should be developed for the United States.

As noted, other countries collect and report many useful statistics. Data on payment fraud collected in Australia, France, Spain, and the U.K. is typically created when account holders inform their financial institutions of an unauthorized transaction. As part of its internal fraud management system, a financial institution would place a marker on the computer record of the transaction indicating that it is fraudulent. The financial institution might also classify the source of the fraudulent transaction, such as from a lost or stolen payment card or from a counterfeit card. Based on computer records, the financial institution can document the number and value of fraudulent transactions for a given time period. This method is able to track gross fraud losses as first reported to financial institutions.

A sponsoring group organizes a method for gathering information from financial institutions and processes the information into aggregate statistics. If nearly all financial institutions are in the reporting system, the aggregate statistics will be representative. One important setup cost is to standardize reporting among financial institutions. Trends in payment fraud would be apparent if the sponsoring group reports aggregate statistics on a regular basis.

While there are no aggregate statistics on payment fraud in the United States, industry groups, consulting firms, and payment processors collect and report fraud statistics on various elements of the payment system. The accompanying table lists some of the more prominent sources and the associated coverage, time period, and payment instrument. Each of these sources asks respondents to report the incidents and losses on

Sources for payment fraud loss statistics in the United States

Source	Coverage	Time period	Payment instruments
Association of Financial Professionals	Medium to large corporations	Annually since 2005	Checks, consumer debit and credit cards, corporate purchasing cards, automated clearinghouse payments, wire payments
American Bankers Association	Small to large banks	Periodically since 1991	Checks and debit cards
CyberSource	Online merchants	Annually since 2000	Primarily debit and credit cards
Javelin Strategy & Research	Consumers	Annually since 2004	Checks, debit and credit cards
PULSE EFT Association	Debit card issuers	Periodically since 2005	Debit cards

Notes: all of these sources use surveys to collect data. PULSE EFT Association sponsors the survey of debit card issuers, which has been conducted by various consulting firms.

payment fraud they have suffered. Other details differ from survey to survey.

In addition, alternative sources for payment fraud statistics include the financial statements of payment providers (which may report fraud losses) and reports prepared by payment providers, such as Visa or MasterCard, which develop statistics based on information provided by their clients. Statistics from these alternative sources are reported on an irregular basis in media publications.

Available sources on payment fraud for the United States are at a disaggregated level and, for various reasons, are incomplete. Many use survey methods that target specific groups of interest and, as a result, will be narrowly focused. The groups covered may overlap and some groups are absent. Time periods vary among sources, as do the types of payment instruments included in the survey. The documentation is not always complete, which raises the possibility of incomparability across time and payment instrument. Finally, important information related to how payment fraud occurs is often unavailable.

In principle, it would be possible to use this disaggregated data to collect information on out-of-pocket fraud losses borne by all payment participants and add them up to get aggregate fraud statistics. At present, however, this would be difficult for the United States because of incomplete coverage of all payment participants in existing sources and because the definition of losses due to payment fraud can differ among sources.

Replicating the system used in other countries to collect and report statistics on aggregate payment fraud, however, would be neither difficult nor excessively burdensome in the United States. Their system relies on data that already exists in many financial institutions. A standardized report would simplify collecting and reporting the statistics. Because the information is confidential and sensitive, financial institutions would be reluctant to release data on payment fraud. A common way to circumvent this concern would be to allow industry control and ensure anonymity by designating an industry-controlled organization to collect and report the data.[13]

Such a system could provide valuable information on the source of payment fraud, the location of fraud, fraud rates by type of payment instrument, and additional statistics.[14] Other major countries have evidently found that the cost-benefit ratio is worthwhile and have stepped forward to provide this information. Whether the same will happen in the United States is an open question.

Endnotes

[1]In mid-September, the list of publicly disclosed data breaches for 2009 compiled by the Identity Theft Resource Center (www.idtheftcenter.org) reports that 376 data breaches occurred in the United States. As of September 2009, BankInfoSecurity reports that one of the breaches, at Heartland Payment Systems, impacted over 670 financial institutions, with many issuing new payment cards of their customers (see www.bankinfosecurity.com/articles.php?art_id=1200).

[2]An example of improved payment security is the payment smart card which is being adopted in many countries. See Richard J. Sullivan, "Can Smart Cards Reduce Payments Fraud and Identity Theft?" Federal Reserve Bank of Kansas City *Economic Review*, Third Quarter 2008 (kansascityfed.org/PUBLICAT/ECONREV/PDF/3q08Sullivan.pdf).

[3]See, for example, Edgar, Dunn & Company, "Payments Risk and Fraud Management: The New World Order," February 2007.

[4]The estimated number of identity fraud victims, most of whom suffered payment fraud, was 9.9 million consumers, a 22 percent increase over the previous year. See Javelin Strategy & Research, *2009 Identity Fraud Survey Report*, 2009.

[5]Association for Financial Professionals, "2009 AFP Payments Fraud and Control Survey," March 2009 (www.afponline.org).

[6]Thomas Glaessner, Tom Kellerman, and Valerie McNevin, "Electronic Safety and Soundness: Securing Finance in a New Age," Working Paper Number 26, The World Bank, 2004, pp. 23-24.

[7]Hitachi Consulting, "2008 Study of Consumer Payment Preferences," September 2008.

[8]Bell, Catherine J., Jeanne M. Hogarth, and Eric Robbins, "U.S. Households' Access to and Use of Electronic Banking, 1989-2007." *Federal Reserve Bulletin*, Vol. 95, 2009.

[9]**Australia:** Australian Payments Clearing Association (APCA) Media Release, "Payments Fraud in Australia," May15, 2009. **France**: Observatory for Payment Card Security (OPCS), *Annual Report*, various issues. **Spain**: ServiRed, Annual Report, 2007 and 2008. **UK**: Association for Payment Clearing Services (APACS), "Quarterly Statistical Release," May 15, 2009; APACS, "Fraud :The Facts," 2009.

[10]The chart shows fraud rates for payment cards because they are reported for each country. Australia and the U.K. also report information on check fraud (not in chart). Statistics for particular years in some countries are unavailable.

[11]For a useful analysis of international differences in fraud rates on these statistics, see Peter Welch, "Online and Overseas: Payment Card Fraud—France, Spain & U.K.," *European Card Review*, December 2008.

[12]EC Staff Working Document, "Report on Cross-Border E-Commerce in the EU," May 3, 2009. A recent survey of consumers in the United States found that 83 percent of consumers made purchases on the Internet (Hitachi Consulting, "2008 Study of Consumer Payment Preferences," September 2008).

[13]Examples are the Australian Payments Clearing Association or the U.K. Payments Administration (formerly APACS).

[14]An ideal payment fraud tracking system would periodically report the distribution of losses among payment participants to help understand several important policy issues. The distribution of losses, for example, can serve as guidance on how to coordinate security efforts. In addition, incentives to take measures to prevent fraud will be directly tied to the actual losses that occur. As a result, changes in liability rules that can shift losses among payment participants will have important effects on the amount of effort to prevent payment fraud.

Collecting the information from existing reporting systems of financial institutions would not be easy because it would require tracking disposition of the loss after it is reported. Another option would be to develop standardized surveys and periodically collecting information for all major groups who bear some losses from payment fraud.

payments system research

Website: *www.kansascityfed.org/home/subwebs.cfm?subweb=9*

The Payments System Research function of the Federal Reserve Bank of Kansas City is responsible for monitoring and analyzing payments system developments. Staff includes:

Terri Bradford
Payments System Research Specialist
Terri.R.Bradford@kc.frb.org
816-881-2001

Fumiko Hayashi
Senior Economist
Fumiko.Hayashi@kc.frb.org
816-881-6851

Christian Hung
Research Associate II
Christian.Hung@kc.frb.org
816-881-4721

Paul Rotilie
Research Associate II
Paul.Rotilie@kc.frb.org
816-881-2357

Rick Sullivan
Senior Economist
Rick.J.Sullivan@kc.frb.org
816-881-2372

Zhu Wang
Senior Economist
Zhu.Wang@kc.frb.org
816-881-4742

Stuart E. Weiner
Vice President and Director
Stuart.E.Weiner@kc.frb.org
816-881-2201