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

Identity Theft: Where Do We Go From Here?*

A Discussion Forum Sponsored by the Payment Cards Center and the Gartner Fellows Program

Julia S. Cheney

April 2004

Summary: *On Tuesday, February 10, 2004, the Payment Cards Center of the Federal Reserve Bank of Philadelphia, in conjunction with the Gartner Fellows Program, hosted a one-day forum titled "Identity Theft: Where Do We Go From Here?" The Center invited participants from the financial services and merchant industries, Internet service and technology providers, and regulatory and law enforcement agencies to discuss key developments facing the credit card and payments industries as they work to combat this growing financial crime. This paper provides highlights from the forum 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

Identity theft is a growing financial crime that affects many segments of our society – consumers, merchants, and credit providers, among others – with direct financial losses. In addition, consumers, in particular, are faced with significant indirect costs stemming from the compromise of their credit files. Such injurious consequences have led to heightened consumer concern about the security of personal information and the price of financial relationships. Credit card companies and others in the consumer payments business are especially vulnerable to any such erosion of consumer confidence.

The Payment Cards Center, in conjunction with the Gartner Fellows Program,[1] sponsored the forum titled "Identity Theft: Where Do We Go From Here?" on February 10, 2004. The forum brought together participants from the financial services and merchant industries, Internet service and technology providers, and regulatory and law enforcement agencies to examine the state of identity theft from each of their viewpoints. The Payment Cards Center sponsored this forum as part of its mission to add insight and to communicate on issues central to the payment cards industry.[2]

Further motivation for the study of identity theft developed from an earlier Payment Cards Center workshop on the subject with Avivah Litan, vice president and research director of Financial Services at Gartner. Among the topics discussed in the workshop was the absence of a common taxonomy among stakeholders on issues associated with the crime.[3] This apparent lack

---

[1] According to Gartner Inc.'s web site, http://www.gartner.com, Gartner, Inc. "is a research and advisory firm that helps more than 10,000 clients leverage technology to achieve business success. Gartner's businesses consist of Research, Consulting, Measurement, Events and Executive Programs. Founded in 1979, Gartner is headquartered in Stamford, Connecticut and has over 3,800 associates, including approximately 1,000 research analysts and consultants, in more than 75 locations worldwide. Fiscal 2002 revenue totaled $888 million."

[2] See the Payment Cards Center's web site www.phil.frb.org/pcc/index.html to obtain additional information on its mission and programs as well as to access the Center's discussion papers, working papers, and the conference agenda.

[3] See Payment Cards Center Discussion Paper "Identity Theft: A Pernicious and Costly Fraud," December 2003, for a review of identity theft and its impact on our payments system and an analysis of its overall costs to consumers, merchants, and credit providers.

of clarity highlighted the need to convene a broad cross-section of industry and regulatory participants in order to construct a common framework for developing effective solutions. The forum was intended as such a platform for these diverse groups to examine initiatives currently underway and to identify possible areas for cooperation among this diverse set of stakeholders.

To encourage open and interactive dialogue among the participants, the forum was loosely structured, and discussion focused on topics raised through four informal panel sessions.[4] The first session, "Taxonomy of Identity Theft and Payment Fraud," was led by Litan and her Gartner colleague John Pescatore, vice president and research fellow for Internet Security. Together, they moderated an exchange among the participants that set a baseline for the day's discussions. In this session, participants considered the definition of identity theft and examined the scope, criminal patterns, and incentives associated with this crime.[5]

The second and third sessions, "Perspectives from the Financial Services Industry" and "Perspectives from Internet Merchants and Service Providers," invited representatives from these industries to assess the identity-theft problem and to review current efforts to limit its financial impact. Additionally, each of these panels considered whether available authentication technologies were viable. Peter Burns, vice president and director of the Payment Cards Center, moderated the banking panel that included the industry fraud experts: Daniel Buttafogo of Juniper Bank, Michael Cunningham of Chase Cardmember Services, Drew MacDonald of Fleet Credit Card Services, and Lyn Porter of Experian Fraud Solutions. Pescatore moderated the Internet merchant and service providers panel that included Christopher Bubb of AOL, Michael Cook of ID Analytics, Steven Klebe of CyberSource, and Howard Schmidt of eBay.

Finally, the last session, "Regulation and Enforcement Targeting Identity Theft," reviewed current policy and law enforcement initiatives in place, or in process, to protect

[4] Refer to page 21 of this paper for a listing of the moderators and panelists.
[5] Much of the material covered in this session can be found in the aforementioned Payment Cards Center Discussion Paper "Identity Theft: A Pernicious and Costly Fraud."

consumers from the substantial and adverse impact of identity theft. This discussion centered on the identity-theft provisions in the Fair and Accurate Credit Transactions Act of 2003 (FACT). Lois Greisman, associate director for the Division of Planning and Information at the Federal Trade Commission (FTC), moderated this panel, which included her FTC colleague Joanna Crane, Assistant U.S. Attorney Richard Goldberg, Amy Friend of the Office of the Comptroller of the Currency (OCC), and Oliver Ireland of Morrison & Foerster, LLP.

Among the many points covered during these panel discussions, three general themes emerged:

- The definition and scope of identity theft and its impact on solutions;
- The efforts to track identity theft and to share data with law enforcement agencies; and
- The role of government in protecting the victim of identity theft.

This paper highlights various aspects of these themes as they developed throughout the day. As is common in any discussion of new and emerging issues, a number of important questions were raised over the course of the day. The paper concludes with a list of these open issues and questions, which we hope will foster a spirit of collaboration among the various parties as they continue working toward solutions.

President Santomero's Opening Remarks

The president of the Federal Reserve Bank of Philadelphia, Dr. Anthony M. Santomero, opened the forum by welcoming the participants and thanking them for gathering at the Federal Reserve Bank of Philadelphia to discuss this complex crime that affects such a wide range of market and policy constituencies. Santomero underscored the seriousness of identity theft: it is a crime that has grave consequences for the victim, merchant, and credit provider, and perhaps more fundamentally, it is a potential impediment to recent advances in our payment systems. The increase in consumer acceptance of a wide variety of more efficient and flexible electronic

payment vehicles is in large part due to consumer trust — developed over a considerable period of time — in the reliability and security of such vehicles. Santomero suggested that identity theft may indeed be a threat to this consumer trust and, therefore, to the advancement of these forms of electronic payments. In summary, he noted that the assembled group offered a rich assortment of expert perspectives that, although diverse, had a common starting point for the day's discussions: a shared sense of purpose to protect victims, to advance our payment networks, and to minimize the social costs of identity theft.

The Definition and Scope of Identity Theft and Its Impact on Solutions

Litan's objective, as she began the first session, was to set a baseline for the day's discussions by establishing agreement on a definition of identity theft. It quickly became evident that the term engendered different interpretations and, notably, it was not consistently applied by the forum participants. Generally, industry participants employed a narrow definition while regulators and law enforcement assumed a broad application of the term. Recognizing this variance and incorporating the differences into the dialogue helped to better focus discussion on solutions.

The narrow definition of identity theft, typically employed by the industry participants, describes this behavior as the wholesale assumption of a person's identity and the use of such identity and associated personal data to establish <u>new</u> credit accounts. To underscore, the trigger for inclusion under the narrow term is that stolen personal information results in access to new credit. Notably, this definition excludes "traditional payment fraud," which stems from the misuse of existing credit account data. For example, traditional payment fraud involving credit cards occurs when thieves use stolen account data, primarily credit card account numbers, to obtain cash or goods. In effect, industry participants' definition derives from the operational need to respond with detection and recovery tactics that can differ significantly, depending on the type

of fraud. At the same time, these participants emphasized that a primary objective of their firms is to minimize losses associated with all forms of fraudulent activity.

In contrast, the broad definition used by regulators and law enforcement agencies does not distinguish among types of fraud that involve compromised consumer information, whether it be a single account number or an individual's entire financial identity. Furthermore, this broad definition extends beyond the financial services industry to include other affected industries, such as telecom companies or Internet service providers. Importantly, this definition follows the codification language in the Identity Theft and Assumption Deterrence Act of 1998. This act makes it a federal crime when someone "knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal Law, or that constitutes a felony under any applicable State or local law." As it relates to the broader definition of identity theft, the act defines a "means of identification" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual."[6] The definition includes several specific terms, notably "access device," which is listed as it is defined in 18 U.S.C. section 1029(e), to mean "any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument)."[7] Therefore, the act's language dictates that identity theft, as a codified term, is more than using stolen identities to create new credit accounts. Indeed, it encompasses a broad

[6] The Identity Theft and Assumption Deterrence Act of 1998 can be found on the Federal Trade Commission's web site at www.ftc.gov/os/statutes/itada/itadact.htm.
[7] http://uscode.house.gov/DOWNLOAD/18C47.DOC -- 18 U.S.C. section 1029(e)

range of fraudulent activity, including — most notably for the forum's discussion — traditional payment fraud.

An important distinction between identity theft associated with the creation of new credit and the traditional payment fraud — misuse of existing accounts — is the former's significantly greater impact on the victim. This increased damage arises mostly as a result of the longer time it takes victims to detect identity theft that involves new credit accounts. Such fraudulently established credit accounts are often associated with address and telephone contact information that is not linked to the victim but of course is accessible to the thief. Therefore, early detection of this crime is difficult because the victim does not receive related account information — such as monthly statements or marketing materials — that would raise a red flag. Typically, such fraud is identified only after a victim has reviewed credit report data or received calls from collection agencies related to these accounts. Conversely, with fraud that involves existing accounts, the account contact data remain tied to the victim, and thus, inaccuracies can be quickly identified through the review of monthly statements. This relatively rapid identification allows for prompt remedial action that generally includes canceling the card to prevent further criminal misuse. Further, federal law limits a victim's liability for payment fraud to $50 per card, and in any case, this fee is generally waived by credit providers. Importantly, existing-account fraud typically involves only a single account, and perhaps a few fraudulent transactions occur before the fraud is discovered and the card canceled. On the other hand, the longer discovery period associated with new-account identity theft allows these accounts to be systematically exploited, such that the fraud losses can become significant, involve multiple accounts, and, ultimately, result in costly and time-consuming efforts to re-establish the victim's credit standing. The recent FTC "Identity Theft Survey Report"[8] captured this loss disparity in its survey results, which indicated that new-

[8] The Federal Trade Commission's *Identity Theft Survey Report* was released in September 2003 and is available at the Federal Trade Commission's web site at http://www.consumer.gov/idtheft. The FTC survey characterizes three types of identity theft: "New Accounts and Other Frauds," "Misuse of Existing

account identity theft, when compared with traditional payment fraud, represented more than two times the cost to businesses and more than three times the cost to victims.

During their respective panel sessions, participants from the Internet service provider and financial services industries expanded on the rationale behind their industries' application of a narrow definition. Christopher Bubb, of AOL, noted that Internet service providers differentiate among fraud associated with identity theft because, by doing so, they are more effective in limiting each variation of this fraud at the operational level. Danny Buttafogo, of Juniper Bank, further stated that breaking identity theft into component parts enables financial services providers to respond specifically to each fraud type. This disaggregation gives lenders the ability to treat each type of fraud with methods that not only address the distinctive attributes of the fraud but also, and more important, have been fine-tuned over time. Buttafogo admitted that the industry is more successful at limiting exposure to some types of fraud than to others, but, he noted, this is typically a result of developing industry experience with new or improved forms of fraudulent activity.

Michael Cunningham, of Chase Cardmember Services, concurred and added that marketing channel, business model, and campaign objective also influence the financial services industry's fraud risk assessments and counter-measures. Marketing channel refers to the consumer contact method, be it direct mail, Internet, or take one.[9] Business model speaks to the client focus, whether it is on consumer or small-business accounts and prime or sub-prime borrowers. Campaign objectives vary and might focus on account acquisition, balance transfers, or convenience check mailings, among others. All of these business applications, in any

---

Credit Cards or Card Numbers," and "Misuse of Existing Non-Credit Card Accounts or Account Numbers." The FTC report compared new-account identity theft — the first type — to total existing-account identity theft (both credit card and non-credit card) – the sum of the second and third types. See pp. 6-7.

[9] In this context, marketing channel refers to the mechanism used by an issuer to contact the customer either for an offer of new credit or as part of the issuer's relationship management efforts. Direct mail is a piece delivered through the U.S. postal system; Internet is an offer delivered via the World Wide Web; and

combination, can have distinct fraud risk exposures. For example, a pre-approved[10] direct mail account-acquisition campaign exposes an organization to different fraud risks and to a lower level of risk than does an un-targeted Internet-based account-acquisition campaign. By considering this kind of detail, Cunningham noted that financial services firms are able to apply prevention strategies that are triggered by specific attributes and that are commensurate with the implied exposure.

Further, Alan Nevels of ICBA Bancard suggested that the size of the institution may also play a role in determining counter-measures, and he referred to community banking organizations as examples. He noted that community banks typically have a stronger personal relationship with their customers and, as a result, have experienced a lower level of fraud than larger institutions. Nevertheless, he suggested that community banks may present a target for identity thieves because many small banks have not had to make the investments in fraud protection technologies that are commonplace in larger organizations.

In summary, many industries take a complex, multi-layered approach to managing fraud risk. Different tools are employed in dealing with specific fraud types and in managing affected relationships. This is especially true as it relates to the counter-measures employed to fight new-account identity theft versus the far less complex issues surrounding the misuse of existing credit accounts. Clearly, forum participants recognize that all fraud risks must be managed, but Cunningham and several other industry participants argued that an increased focus on new-account identity theft is also required. They reasoned that credit providers, regulators, law enforcement agencies, and particularly consumers will be more successful in pursuing their common goal of curtailing crimes associated with new-account identity theft if there is a clear

---

take one is a physical application that customers pick up at designated locations and take with them to complete.

[10] Campaigns may be pre-approved or not. Pre-approval is a process by which an issuer is able to obtain a list that includes only prospects that meet certain pre-defined criteria, such as having a FICO score above 640.

understanding of the differences between the various fraud types and the need for tailored remedies.

Joanna Crane, of the FTC, noted that her agency has recognized some of this complexity in defining identity theft. In fact, the FTC intentionally structured its recent survey to allow for the delineation of the results between the misuse of existing accounts — traditional payment fraud — and the establishment of new credit accounts, as per the industry's more specific definition. The FTC survey report estimated identity theft's total losses to businesses and consumers to be $47.6 billion and $5.0 billion, respectively. This total includes business losses of $32.9 billion related to the establishment of new credit accounts and business losses of $14.0 billion related to misuse of existing accounts. Consumer losses were broken out in this same manner. For consumers, $3.8 billion related to the establishment of new credit accounts and $1.1 billion related to misuse of existing accounts.[11] Crane emphasized that the financial losses to both businesses and consumers, regardless of whether the narrow or broad definition was applied, were significant and greater than had been previously estimated using its consumer complaint system as a proxy.[12]

The question arose as to whether this definitional distinction hindered effective, ongoing communication between the industry constituencies and the regulators as they move toward solutions. After much discussion, Lois Greisman, of the FTC, suggested that perhaps the definitional debate is not the real roadblock, and in fact, such debate may be primarily about semantics. At the end of the day, the greater need is for regulators and industry stakeholders to continue dialogue, particularly as FACT legislation moves toward the rulemaking phase of implementation. The heart of success will lie in whether the new guidelines and rules will

[11] See the Federal Trade Commission's *Identity Theft Survey Report*, p. 7

[12] The FTC established the Identity Theft Data Clearinghouse, part of the Consumer Sentinel System, to track consumer complaints regarding identity theft. For more information on this system, see the FTC's web site at http://www.ftc.gov/bcp/conline/pubs/general/idtheftfact.htm.

effectively protect consumers from the long-term and pernicious effects of new-account identity theft and, at the same, continue to provide credit providers with the flexibility to best detect and mitigate financial fraud in all its forms.

Efforts to Track Identity Theft and to Share Data with Law Enforcement Agencies

Assistant U.S. Attorney Richard Goldberg emphasized that from the law enforcement perspective, the definition of identity theft is not important because, to investigative agencies, all fraud is a crime with a victim, regardless of what the crime is called. Rather, Goldberg stressed that the challenges faced by fraud investigators are resource related. He noted that fraud crime investigations, particularly those associated with identity theft, are complicated by the extent to which personal data are accessible in our society. Many organizations — banks, Internet service providers, hospitals, universities, and telecom companies, among others — have valid business reasons to obtain personal data as part of their customer, student, or employee relationship. Goldberg pointed out that investigators must not only examine each "user" of personal data but also each exchange of personal data and the parties who had access to the personal data during such an exchange. Therefore, these investigations present what Goldberg called a significant number of "compromise points," each of which requires due diligence by a limited number of investigators.

Goldberg suggested that organizations with access to personal data can take several steps to help improve investigative efficiencies for law enforcement agencies. Preventive measures, such as establishing proven data-protection protocols, can add controls around the compromise points. At the same time, organizations can assist law enforcement in the recovery process by improving the tracking and reporting of incidences to law enforcement agencies. Finally, the establishment of a universal database that includes cross-industry incidence reporting and is

accessible by all levels of law enforcement – federal, state, and local – will assist these agencies in coordinating and targeting investigative efforts.

Participants agreed that data sharing is crucial to making progress in the fight against identity theft, and discussion included several initiatives underway by various organizations. All of these initiatives have the common focus of providing law enforcement agencies with easier access to incidence-tracking data.

Foremost among these efforts have been those made by the FTC as part of fulfilling its directive under the Identity Theft and Assumption Deterrence Act of 1998. This act specifically directs the FTC to establish a central complaint system to receive complaints about identity theft and refer them to appropriate entities, including law enforcement agencies and national credit reporting agencies. As a result, the FTC has been instrumental in leading data-sharing efforts through its implementation of a three-pronged approach that Joanna Crane briefly summarized in her remarks. The first effort established a means by which victims can report the crime: an FTC-sponsored telephone hotline and web site. The second enabled tracking of consumer complaints made via the telephone hotline or the web site in the Identity Theft Data Clearinghouse. This clearinghouse allows the FTC to share aggregate information with consumers, government agencies, and industry constituencies. Further, it provides law enforcement agencies with direct access to detailed incidence data on a case-by-case basis. Last, the act directs the FTC to educate consumers about the risks associated with identity theft and protection strategies that consumers can employ to safeguard their personal data.[13] From the inception of the FTC's Identity Theft Data Clearinghouse in November 1999 through December 2003, the system had logged almost

[13] For a fuller description of the FTC's directives, see commission testimony titled "Identity Theft: Prevention and Victim Assistance," given before the Subcommittee of Oversight and Investigations of the House Committee on Energy and Commerce, December 15, 2003, pp. 1-3. Full testimony is available at http://www.ftc.gov/os/2003/12/031215idthefttestimony.pdf.

500,000 consumer complaints.[14] In July 2000, law enforcement agencies gained access to this database for their use in investigations and prosecutions. Since then, more than 670 federal, state, and local law enforcement agencies have registered with this database, and over 4,200 individual agents have desktop access to the database.[15]

Additional data-sharing efforts are being developed at local levels. Assistant U.S. Attorney Richard Goldberg leads the Regional Identity Theft Working Group in Philadelphia, Pa. This group meets to share information about regional cases worked by the group's members, including federal, state, and local investigative agencies. He noted that similar working groups are being created in several districts around the country, and the identity theft database developed in Philadelphia may eventually be used in other places. In this way, the regional working groups are able to correlate local cases with national trends, to coordinate investigative efforts with other regional initiatives, and to address issues of jurisdiction.

Both Greisman and Goldberg agreed that the piece historically missing from the Identity Theft Clearinghouse data set has been incidence data from affected companies across those industries typically targeted by identity thieves, most notably banks but also including telecom companies, hospitals, universities, and Internet service providers, among others. Access to such information would improve law enforcement's ability to identify broader criminal patterns and to allocate its investigative resources.

Greisman highlighted a recent industry initiative advanced by the Financial Services Roundtable's technology arm, BITS,[16] and its members as an example of progress in the arena of data tracking and sharing between affected companies and law enforcement agencies. She noted

---

[14] See "National and State Trends in Fraud and Identity Theft January – December 2003," p. 9. The report is available at http://www.consumer.gov/sentinel/pubs/Top10Fraud2003.pdf.
[15] See "Federal Trade Commission Overview of the Identity Theft Program: October 1998 – September 2003," pp. 3-5, 8. The report is available at http://www.ftc.gov/os/2003/09/timelinereport.pdf.
[16] The Financial Services Roundtable's web site can be found at www.fsround.org and includes links to the BITS web site. It also provides descriptions of the mission and membership of both organizations.

that the Financial Services Roundtable and BITS have created the Identity Theft Assistance Center (ITAC) to streamline the notification process for victims and to provide incidence-tracking data to law enforcement agencies. As initially planned, ITAC will give victims the ability to register an incidence of identity theft once with their primary financial institution and to direct that financial institution to forward the information to ITAC. ITAC will then complete the notification process by informing the victim's other credit providers that fraud may have occurred. Importantly, BITS has been working with the Federal Trade Commission and law enforcement agencies to develop procedures for uploading such data into the FTC's Identity Theft Data Clearinghouse to facilitate law enforcement agencies' direct access to these data. The Identity Theft Assistance Center pilot program is expected to be operational by the second quarter of 2004.[17]

Michael Cook, of ID Analytics, presented another industry effort. His firm completed a one-year study that analyzed identity-theft fraud occurring in several industries, including wireless providers, retail banks, and credit card issuers. This study provided a view of the criminal pattern of identity theft across these industries and helped ID Analytics in its development of tools aimed at predicting the likelihood of identity theft at the point of the initial application for credit. ID Analytics' goal is to provide application scoring that assists companies in preventing identity theft before it happens.[18]

Howard Schmidt, of eBay, discussed another effort related to information sharing that some companies in the technology industry are employing to address identity theft. Essentially, firms are supporting informal gatherings of their top information security personnel in order to

[17] BITS press release "New Center to Assist Victims of Identity Theft and Reduce Fraud," dated October 28, 2003, can be found at http://www.bitsinfo.org/bitsitacoct2803.pdf and the BITS press release "Leading Financial Institutions Form Identity Theft Assistance Corporation," dated January 29, 2004, can be found at http://www.bitsinfo.org/bitsitacjan04.pdf

[18] ID Analytics press release "ID Analytics Announces Findings from Largest-Ever Research into Identity Fraud with Cooperation of Business Leaders Across Multiple Industries," dated September 23, 2003, can be found at http://www.idanalytics.com/news_and_events/20030923.html

share information about new or improved methods that thieves are using to steal personal information and commit fraud. These informal exchanges allow participants to keep up with the rapidly changing methods used by computer-savvy criminals. Schmidt noted that this approach enables each firm to more quickly implement counter-measures to protect consumer data and to reduce associated fraud losses. Importantly, Schmidt noted that law enforcement agencies are also included in these gatherings. In this way, the technology industry shares information regarding changing criminal behavior patterns with law enforcement agencies so that industry insights can be incorporated by these agencies into their investigative processes.

In summary, although government and industry organizations are taking many steps to improve law enforcement agencies' access to identity theft incidence-tracking data, resource constraints remain a challenge. The number of industries affected combined with the number of compromise points requires a prioritization of available resources that limits the extent to which agencies can investigate this form of criminal activity. Consolidation of incidence data into an aggregated reporting platform by affected industries – banks, telecom companies, Internet providers, and so forth – can aid law enforcement agencies' efforts to identify criminal patterns, recognize the crime sooner, and prosecute identity thieves. But clearly, the threat of criminal prosecution on its own is not a sufficient response to identity theft and must be accompanied by action from all stakeholders to protect personal data and thereby to prevent the initial victimization.

The Role of Government in Protecting the Victim of Identity Theft

In discussing prevention efforts earlier in the day, Litan outlined the incentives influencing consumers, merchants, and lenders in addressing this crime and reducing its overall effect on each party. In her analysis, consumers face significant costs when victimized by identity

theft and are the most motivated to reduce the incidence and impact of this crime. At the same time, the consumer has limited individual power to do so.

Ollie Ireland, of Morrison & Foerster, LLP, noted that recent FACT Act legislation included identity-theft provisions that will go a long way toward providing consumers with tools to assist in personal data protection, credit data monitoring, and credit score recovery. In particular, he cited provisions that allow consumers to receive a free annual credit report from each of the national credit reporting agencies and to flag accounts on credit files that are suspected of being fraudulent. Further, he noted the legislation requires lenders and credit reporting agencies to take preventive and recovery steps.

Amy Friend, of the OCC, spoke to this point by citing a key aspect of FACT identity-theft legislation: the provisions requiring federal banking agencies, the National Credit Union Administration, and the Federal Trade Commission to jointly establish "red-flag" guidelines and rules related to identity theft for entities subject to their enforcement. Friend outlined these general requirements:

- To establish and maintain red flag guidelines for financial institutions and creditors regarding identity theft. The patterns, practices, and specific forms of activity that indicate the possible existence of identity theft are to be identified as the banking agencies develop these guidelines. Further, banking agencies should consider including guidelines specific to a change in status for accounts that have been inactive for more than two years because a request for such a change may indicate an attempted identity theft.
- To stipulate regulation that requires financial institutions and creditors to establish reasonable policies and procedures to implement the above guidelines.

- To prescribe regulation governing a change-of-address request according to specific policies and procedures as described in more detail in the statute. [19]

Friend noted that regulators are facing a number of challenges in establishing these guidelines and rules. As previously described, the varying definitions of identity theft are problematic in terms of calibrating rules and guidelines to protect consumers without placing undue strain on the efficiency and smooth functioning of our credit markets. Specifically, determining guidelines and rules that support fraud counter-measures will be crucial. In this vein, Friend suggested that such efforts may require consideration of a number of factors, such as the size of the financial institution or creditor, combined with some form of risk-based approach that recognizes such nuances as marketing channel, business model, and campaign objective. A consensus emerged in the discussion that in order to successfully implement FACT Act legislation, industry representatives and regulators must continue working together to effectively develop these guidelines and rules through the notice and comment period.

The FACT Act also places additional responsibilities on credit reporting agencies (CRAs). Lyn Porter, of Experian, emphasized that CRAs are in a novel position because FACT legislation puts significant responsibility on CRAs to assist consumers who are, in fact, customers of CRA clients rather than of the CRA itself, in managing credit report data and in navigating the dispute and re-investigation processes. For example, Porter noted that CRAs will now be required to notify creditors when a request for a consumer report includes an address for that consumer that differs substantially from the address in the consumer's file. This is in addition to the provision requiring a one-call process allowing consumers to call any nationwide CRA and add a fraud alert to their file. These alerts must be shared with the other nationwide CRAs. Also, she reiterated the requirement to provide consumers with a free credit report annually. As she and a

[19] For additional detail, see H.R. 2622, Fair and Accurate Credit Transactions Act of 2003, Section 114

number of the participants noted, the FACT Act requires CRAs and others to assume costs, which may be significant, associated with FACT's provisions and that the ultimate impact of these costs on consumer credit is uncertain.

Howard Schmidt and Christopher Bubb pointed out another area, aside from consumer protection, in which the government may have a role to play: supporting authentication technology standards and encouraging consumers to adopt this technology. Indeed, under the FACT Act, the secretary of the Treasury is charged with conducting a study on the use of biometrics or similar technologies as identity authentication tools to reduce the incidence and cost of identity theft.[20] Consumers' ability to authenticate their identities in either an online or brick-and-mortar environment offers additional validation that the transactor is indeed the individual represented by the personal data. Steven Klebe, of CyberSource, noted that several new authentication tools exist, such as Verified by Visa and MasterCard SecureCode, but that these technologies have not yet been widely adopted by merchants or consumers. He explained that these technologies require customers to enter a password during the checkout process, slightly slowing the process down. Additionally, he pointed out that if these technologies are not implemented well, rates of abandonment could increase. As a result, merchants are hesitant to implement authentication solutions that are not ubiquitous and that do not offer enough economic incentives to offset the potential negative impact on customer satisfaction and sales.

Schmidt argued that protecting personal data is not just the purview of government and industry; consumers also have a responsibility to participate in the process of protecting their personal information. Buttafogo agreed and stated that banks could be better positioned to protect consumer data if consumers were more receptive to available authentication technologies. He cited the example of voice authentication and noted that, in tests, very few consumers were willing to take the time to register their voices. In response, Klebe noted that changing consumer

[20] For additional detail, see H.R. 2622, Fair and Accurate Credit Transactions Act of 2003, Section 157.

behavior is often difficult. In point of fact, Schmidt noted that most consumers still use static user identifications and passwords. Simple consumer efforts, such as shredding personal documents, rotating passwords, and safeguarding personal data, can greatly aid industry and government in their work to secure personal data. In summary, consideration was given to the possibility that credit providers' success in making it easy for consumers to obtain and use credit and to transact business in new environments may have had an unforeseen result: it established a disincentive for consumers to personally take action to protect their private data.

Both Schmidt and Bubb stressed that the development of a commercially distributable, reasonably priced, and, most important, widely adopted two-factor authentication system will be a watershed advancement for adding security and reliability to the growing e-commerce channel and helping to reduce the incidence and impact of identity theft. Schmidt not only expressed confidence that such a solution was feasible but also predicted its introduction and widespread adoption within the next 12 months. Although this prediction was greeted with skepticism, several participants acknowledged that technological solutions are clearly available and that the challenge resides in the packaging of such solutions to encourage widespread adoption and the setting of a national standard.

Open Issues and Uncertainties

Throughout the day's discussions, forum participants exchanged a range of perspectives on the issue of identity theft. The exchange led the group to conclude that some points of difference among the participants were more easily resolved than others through ongoing communication, and certainly such differences were not roadblocks to solutions. At the same time, participants agreed that other aspects of this issue are more complex and require further consideration by these parties as they continue to work toward solutions. As such, the dialogue

highlighted several issues or uncertainties that were either new or that remained after the day's discussions:

> Given the different definitions of identity theft, can regulatory and industry constituencies work together to establish guidelines and rules that protect consumers from new-account identity theft and, at the same time, continue to allow industry to respond to different types of fraud with specific operational responses?

> Do consumers understand the distinction between new-account identity theft and traditional payment fraud? Is it important to educate consumers about the differences associated with these fraud types? Would greater understanding lead consumers to take more effective prevention measures?

> How can current data-sharing initiatives better incorporate the data from banks and also expand to incorporate reporting from other affected industries? Can such reporting efforts be accomplished through one point of contact, and is that point the FTC Identity Theft Clearinghouse?

> Should FACT guidelines and rules consider a risk-based approach, taking into consideration marketing channel, business model, and campaign objective as well as the size of the institution?

> Assuming that FACT is successful at re-setting market incentives to provide adequate protections to consumers primarily, and to merchants and credit providers secondarily, are the costs of meeting FACT Act identity-theft provisions allocated appropriately among industries or specified parties, for example, credit reporting agencies?

> Does FACT legislation do enough to substantially reduce the impact of identity theft on victims and to require data sharing with and data access to law enforcement?

> Can identity-theft solutions be effective without expecting some personal responsibility in regard to data protection?

> Is a widely adopted, ubiquitous identity security system truly possible in the near term? In any case, what organizations need to participate in the development of such technology?

In conclusion, identity theft is a complex crime necessitating the involvement of many segments of our society in reducing its financial impact on all participants in the payment system. As President Santomero noted, combating identity theft is also necessary to ensure that consumers are confident in their ability to make transactions in a safe and secure payments environment. During the day, participants discussed several efforts that suggest progress is being made in combating this crime. However, in each of the following areas — data-sharing efforts, implementation of FACT legislation, and development of authentication technology — continued coordination among the invited stakeholders is crucial. The effectiveness of each of these initiatives will ultimately be determined by the ability of industry, regulators, and law enforcement to reach agreement on the vulnerabilities in the system that lead to victimization and the ability of these constituencies to establish appropriate responses.

Identity Theft: Where Do We Go From Here?
Sessions and Speakers

Welcome
Dr. Anthony M. Santomero, President, Federal Reserve Bank of Philadelphia

Combating Cyber-age Identity Theft and Payment Fraud:
Taxonomy of Identity Theft and Payment Fraud

Avivah Litan, Gartner Inc.
John Pescatore, Gartner Inc.

Pain Points of Identity Theft and Payment Fraud:
Perspectives from the Financial Services Industry

Moderator: Peter Burns, Federal Reserve Bank of Philadelphia
Panelists: Daniel Buttafogo, Juniper Bank
Michael Cunningham, Chase Cardmember Services
Drew MacDonald, Fleet Credit Card Services
Lyn Porter, Experian Fraud Solutions

Pain Points of Identity Theft and Payment Fraud:
Perspectives from Internet Merchants and Service Providers

Moderator: John Pescatore, Gartner Inc.
Panelists: Christopher Bubb, AOL
Michael Cook, ID Analytics
Steven Klebe, CyberSource
Howard Schmidt, eBay

Regulation and Enforcement Targeting Identity Theft:
Current Initiatives, Successes, and What's Next

Moderator: Lois Greisman, Federal Trade Commission
Panelists: Joanna Crane, Federal Trade Commission
Amy Friend, Office of the Comptroller of the Currency
Richard Goldberg, AUSA (Assistant U.S. Attorney)
Oliver Ireland, Morrison & Foerster, LLP