Testimony of

Michael D. Cunningham

Senior Vice President

Credit and Fraud Operations

Chase Cardmember Services

Tempe, Arizona

Before the

Senate Banking Committee

June 19, 2003

Mr. Chairman, Members of the Committee, my name is Michael D. Cunningham and on behalf of J.P. Morgan Chase & Co., we greatly appreciate this opportunity to appear before the Committee and share our experience with the issue of identity theft. I serve as Senior Vice President for Credit and Fraud Operations for Chase Cardmember Services. Protecting our customers from identity theft and fraud is a major priority for our entire company. We have devoted the resources necessary to play a leading role for the industry by utilizing leading edge technology and hands on intervention by over 750 specially trained Chase employees. The personal security and well being of our customers is a top priority at Chase.

Below, please find a discussion of the problem, the nuts and bolts of what we at Chase do about it, followed by some ideas for changes and improvements for all parties involved.

I. Elements of Identity Theft and Credit Card Fraud

Identity Theft

While identity theft and what we call credit card fraud are both pernicious crimes, and both constitute fraud, we would like to distinguish the two for policy purposes. We place identity theft into two basic categories:

Fraudulent Applications—Three Percent of Our Total Fraud Cases

This involves the unlawful acquisition and use of another person's identifying information to obtain credit, or the use of that information to create a fictitious identity to establish an account.

In order to commit identity theft by means of fraudulent application, the perpetrator needs to acquire not just a name, address or credit card number but unique identifiers such as mother's maiden name, social security number and detailed information about a person's credit history such as the amount of their most recent mortgage payment. This is why more than 40 percent of the identity theft cases that we see are committed by someone familiar to the victim, frequently a family member or someone in a position of intimacy or trust. This variety of identity theft represents three percent of our total fraud cases.

Account Takeover—One Percent of Our Total Fraud Cases

This occurs when someone unlawfully uses another person's identifying information to take ownership of an account. This would typically occur by making an unauthorized change of address followed by a request for a new product such as a card or check, or perhaps a PIN number. This variety of identity theft represents less than one percent of our total fraud cases.

Non-Identity Theft Fraud—The Other 96 Percent of Our Total Fraud Cases

This type of fraud constitutes the vast majority of occurrences and falls under four basic headings:

1) Lost or Stolen Cards: The card is actually in possession of the customer and is subsequently lost or stolen.

2) Non-Receipt: The card is never received by the customer and is intercepted by the perpetrator prior to or during mail delivery.

3) Counterfeiting: The card is in possession of an actual customer and a fraudulent one is subsequently created by a variety of forgery or counterfeiting techniques. The customer does not know that the theft has occurred.

4) Fraudulent Mail or Telephone Order: The card is in possession of the customer and the account number and expiration date is compromised permitting purchases by phone, mail or Internet.

Who Bears the Liability for Fraud?

By law, the liability of the consumer who has suffered credit card fraud is limited to a maximum of $50 up to the time of notification to the creditor, after which it is zero. As a practical matter, with the advent of the Internet and other mediums, to promote consumer confidence, MasterCard and Visa simply accept full liability for the fraud, as do many individual card issuers.

II. The Role of Credit Delivery Systems in Fraud

Variation in Fraud Rates by Application Channel

Table 14: Cost of Credit-Card Fraud[1]

Type	Year 2000 Cost (Millions)	% of Credit Card Fraud	% of Sales Volume
False Applications	$46.1	4.5	0.004
Other Fraud	$976.1	95.5	0.078
Total	$1,013.2	100.0	0.082

During the course of the debate on identity theft and fraud, critics have alleged that the process known as "prescreening" or "prescreened offers of credit" somehow are major contributors to identity theft and other types of fraud. This is

[1] *The Fair Credit Reporting Act: Access, Efficiency & Opportunity, The Economic Importance of Fair Credit Reauthorization*, Information Policy Institute, June 2003, p60.

not the case. In fact prescreening is a major underwriting tool integral to safety and soundness and the lower cost of credit.

Prescreening Greatly Enhances the Ability of Credit Grantors to Accurately Assess Risk and Avoid Losses and Lower Costs

Prescreened offers have a very low incidence of fraud, and especially so when compared with other forms of new account generation. At Chase, for 2002, prescreened accounts subject to identity theft involved approximately 600 accounts measured against 17 million total active accounts. Total fraud cases of all types for 2002 amounted to about 75,000, including the 600 prescreening cases. Last year, prescreening resulted in 1.6 million new accounts out of a total of 4 million new accounts, or 40 percent of all new accounts. Again, the majority of fraud arising from prescreened accounts is committed by someone familiar to the victim. One of our competitors, Capital One, a large user of prescreening, recently testified before the House Committee that they had similar experience, reporting rates of identity theft that are "5 to 15 times lower for credit generated through prescreening than from credit generated through other channels (e.g., the Internet, in-store "take ones")."

Why do prescreened cards result in less identity theft? Prescreened offers of credit come from a pool of consumers selected from credit bureau files that have already undergone a substantial verification and underwriting process. An identity thief or fraudster that is not a family member always chooses the most anonymous method of application such as the Internet, or an in-store "take one" application. Choosing a prescreened credit card application is the most difficult route by far for the thief. Prescreened credit card offers do not contain any personal information other than name and address, and contain none of the other personal information necessary to apply for credit. Identity thieves do not find pre-screened offers of credit very useful because even if they intercept one, they have to submit a change of address, which under Chase's system (and others that we know of) would trigger an alert and subsequent analysis.

The reduced risk of identity theft and other types of fraud has benefits far beyond enhancing the personal security of our customers. This enhancement to the underwriting process lowers the cost of capital and hence the cost of credit and permits more credit to be extended. Without prescreening and other techniques for accurately assessing risk, the costs to credit grantors of raising capital in the secondary financial markets would be increased**.** In order to minimize their costs of capital, major credit card issuers and other credit grantors (*e.g.,* auto lenders) sell a large percentage of their receivables to secondary bond market investors. Many issuers sell up to one half of their receivables to investors in the secondary markets. The models used to price these securities are largely based on the assessment of credit risk. Without the credit enhancements of prescreening (and other national credit standards), these models would almost certainly have to be changed to factor in additional risks of default, resulting in an increase in costs to the issuers of these securities.

III. The Role of the Credit Card Industry as the Early Warning System for Identity Theft and Fraud—Detection, Prevention and Resolution

Industry Practices in General

The recently released report by the Information Policy Institute, contains an excellent description of industry practices in general [2]:

> **Credit card issuers also have authentication procedures in place at many stages of the process to limit the ability of criminals to open fraudulent credit card accounts. The vast majority of credit card issuers (if not all of them) review the application, using a variety of automated tools (Appendix F) based upon credit file data to authenticate the identity of the applicant. In some cases, if the lender has any degree of uncertainty about the applicant's identity, additional documentation (such as a state-issued driver's license, or a utility bill) is requested before approval is granted. Even after the card has been physically delivered to the applicant, the account is not activated until the applicant again verifies his or her identity, usually by calling from his or her home phone.**
>
> **Issuers undertake these procedures because they are generally liable for the cost of fraudulent charges. MasterCard and VISA, for example, have zero liability policies that significantly limit the consumer's responsibility for fraudulent charges. Issuers will soon legally be required to authenticate identity when opening accounts as well. Given the cost to issuers, it's no surprise that losses from fraudulent applications account for significantly less than one-hundredth of one percent of credit card sales volume and less than five 5 percent of all credit card fraud.**
>
> **The vast majority of credit card issuers further review the application using a variety of sophisticated automated tools. These authentication tools check the applications for inconsistencies, compare information from the application to that in credit files and other national databases, and check applications against databases on known fraud. If inconsistencies are detected, or if the application is identified as being high risk for fraud, the tools instruct the issuer to decline the application or perform a thorough manual review.**
>
> **For example, if the applicant attempts to change the address and the new address is different than in these databases, the products indicate the possibility that the application is fraudulent and that an identity thief is trying to open an account and divert mail away from the victim's address to avoid being detected. These products are very successful, identifying the majority, from 60 to 80 percent, of fraudulent applications before the**

[2] *Ibid p.60-61.*

accounts are ever opened. The success of these tools also serves as a powerful deterrent to potential identity thieves.

Prevention and Detection at Chase Cardmember Services

Chase uses a multi-layered system of technology, manual analysis and consumer education and assistance to prevent, detect and resolve all types of fraud. In fact, we detect approximately 70 percent of all fraud before the customer even knows it has occurred, and we continue to improve every year. The first step in this effort is to assess the risk at the application level. Below are some examples of high-risk attributes for an application:

1. Discrepancies between credit bureau and application data. For example we compare, social security number, address, name and date of birth – discrepancies cause rerouting to our manual system.
2. Credit bureau fraud alerts and victims' statements.
3. Internal fraud file matches, which entail matches against key personal identification data in a file that contains prior victims of ID theft.
4. Issuer's Clearinghouse Services (ICS) alerts. The ICS is a shared issuer database of reported ID theft victims.

Low risk applications are automatically approved and monitored for suspicious activity by a specialized unit. High-risk applications are subject to manual verification. This includes:

1. Address validation using a variety of databases.
2. Direct contact with the true person whose name is being used to apply for credit at the location verified for that person.
3. Authentication using "out of wallet" information such as a person's most recent mortgage payment or similar types of information that typically is not found in a person's wallet and that only the true customer would know.
4. Request for documentation from the applicant in situations where we are unable to verify the applicant's identity.

In addition to the above, we have also developed an address change model that utilizes demographic techniques and a file of known fraudulent addresses. Additionally, we have a security verification methodology for special cases such as when an applicant has no home phone number.

Utilizing all of these technologies and human resources, Chase frequently provides the first notice to the consumer of identity theft or fraud. Below is an excerpt from a letter from one of our customers:

> "I would like to take this opportunity to praise the performance of (Chase employee)...Over 6 months ago Mr X called me at home because he noticed a discrepancy in a

credit application that had my name and SS#. He gave me valuable information that minimized the damage to my credit and ultimately led to the arrest of a ring of identity thieves."

Consumer Assistance and Education

At Chase, we recognize that consumers may need help once they learn of the identity theft or fraud. Once a problem is identified, Chase provides consumer education and assistance programs, as detailed in the two documents in the Appendices to this statement. As you can see, we try to be as proactive as possible in dealing with consumers who are victims of identity theft or fraud. We also actively work with law enforcement to try and apprehend the perpetrators. We employ our own investigators who provide a summary report to law enforcement officials. We then file a "Suspicious Activity Report" (SAR) in accordance with federal regulations, and we provide testimony to aid in the prosecution of specific cases.

Technological Tools to Prevent Identity Theft

-

In addition to the detection and prevention methodologies outline above, we employ three important technical tools for prevention of identity theft. First, we use Falcon, a so-called neural network technology, which calculates a "fraud score" for transactions based on data from a consortium of creditors and customer/merchant profiles. Based on this system, we have adopted strategies to approve, decline or refer a transaction for further analysis. Some of the events that may trigger further scrutiny of a transaction or an account include new accounts showing cash advance and jewelry type transactions or a recent address change accompanied by high dollar cash or mail/ phone order activity, just to name two examples.

Second, we also employ a system that we call "link analysis" that utilizes known fraud information to stop subsequent occurrences. This is composed of a caller ID database combined with addresses, home and business phone numbers, social security numbers and a variety of other relevant information to stop ID theft before the perpetrator can assume the identity of an innocent consumer. The third technology that we apply is a fraud application-scoring model that relies on patterns and other criteria to generate a fraud score for a particular transaction. No one approach is a cure-all, but taken together, these applications have enabled a continual improvement in our performance.

IV. Recommendations to Enhance Consumer Protection from Identity Theft and Fraud

In conclusion, despite everything that Chase and others in the industry are doing to combat these types of fraud, we have identified some areas that would benefit from legislative changes. Please find below an outline of technical changes to the

law by category that we feel would assist everyone concerned in the fight against these crimes.

Prevention

(Applicable to Financial Institutions)

- Financial institutions must establish risk-based policies and procedures to verify customer identification information.
- Such policies and procedures used to comply with the requirements imposed under Section 326 of the PATRIOT Act shall suffice for purposes of account opening.
- Such policies and procedures must include the evaluation of a "fraud alert" obtained in connection with a consumer report.
- Such policies and procedures must include address change verifications, as appropriate.
- To the extent not already permitted or authorized, authorize financial institutions and associations of financial institutions to share information with other financial institutions, or associations of financial institutions, regarding individuals, entities, organizations, or transactions that may involve identity theft or possible identity theft. A financial institution or association that transmits, receives, or shares such information for the purposes of identifying and reporting identity theft activities shall not be liable to any person under any law, regulation, or agreement. Extend the same flexibility and protections to other businesses affected by identity theft, such as retailers.
- Require disclosure (at same time as "initial" TILA disclosures) to inform consumers that the financial institution may report information to a consumer reporting agency regarding the consumer's behavior on the account. Disclosure must also provide contact information to consumer reporting agencies that operate on a nationwide basis.
- Allow access to Social Security Administration database in order to verify social security numbers on applications.

Prevention (Applicable to Consumer Reporting Agencies)

- Nationwide consumer reporting agencies must establish a method of recording and reporting "fraud alert" data.
- Consumer reporting agencies may truncate an individual's social security number on copies of the individual's credit report provided to the individual so long as the social security number provided by the individual to obtain the credit report matches the social security number included in the credit report.

Other Prevention Related Measures

- To the extent not already permitted under the FCRA, include fraud prevention and identity theft prevention as a permissible purpose to obtain a consumer report under the FCRA.
- Ensure continued availability of consumer reports as envisioned under the FCRA.

- Prohibit display or sale of an individual's social security number to general public. Such prohibition shall not interfere with legitimate business-to-business or business-to-government transfers of social security numbers, or public record information.
- Prohibit merchants from printing more than the last four digits and the expiration date of a credit card number on a receipt.
- Prohibit states from printing social security numbers on driver's licenses and other government issued form of identification.

Apprehension

- Have postal service hire additional postal inspectors for purposes of identity theft and related investigations.
- Increase penalties and prosecution for identity theft crimes.
- Require the Department of Justice to develop a training program for state and local law enforcement with respect to identity theft crimes.
- Require the Department of Justice to develop model definitions, reporting forms, and affidavits for use by state and local law enforcement in connection with identity theft investigations.
- Improve civil forfeiture provisions related to identity theft.

Mitigation

- Require consumer reporting agencies to block tradelines allegedly the result of identity theft if the consumer provides a valid police report regarding the identity theft [or other valid indicia of the crime] and provides appropriate identification.
- Require a business to provide information to a consumer pertaining to an alleged identity theft if consumer provides a valid police report regarding the identity theft [or other valid indicia of the crime] and provides appropriate identification. This provision must be crafted to ensure it does not create additional opportunities for identity theft, and businesses may not be held liable for complying with this provision.

Victims Assistance

- Develop a simplified standardized document e.g., Uniform Affidavit for consumers' initiation of investigations of claims related to identity theft.
- Simplify the way consumers can contact their financial institution to make a claim of identity theft e.g., call a toll free number on their account statement.
- Be responsive to identity theft claims in a timely fashion.
- Require local law enforcement to accept the simplified standardized form and to assist the consumer and to produce a police report.

APPENDIX A

Education and Outreach Efforts

Chase believes that education and outreach about how to protect oneself from becoming the victim of ID Theft is also important. In support of this belief, we have taken the following educational efforts regarding ID Theft:

a) Tips on protecting your identity & accounts are posted on Chase's Privacy & Security page on www.chase.com

b) Periodic notices are included in our statements for customers regarding prevention of ID Theft.

c) Outreach to the Community through Senior Citizens groups and groups like AARP.

d) Provide advice through toll free numbers to potential victims or persons concerned about what to do, including the providing of an ID Theft Kit.

e) Education is provided to our employees about Safeguarding Customer Information. A training tape was prepared which became the Industry Standard and was provided by the American Bankers Association to all banks. Internal Intranet training about ID Theft prevention and Information Safeguarding is mandatory to all those with access to customer information.

f) Our Code of Ethics includes the rules regarding information use and access. Violators are punished – including dismissal and prosecution.

APPENDIX B

CHASE

THE RIGHT RELATIONSHIP IS EVERYTHING.®

IDENTITY THEFT HELP KIT

TABLE OF CONTENTS

INTRODUCTION

At Chase, we understand how upsetting these circumstances are for you and we want to help. First, Chase will work with you every step of the way to resolve your situation at Chase. Second, we will assist you as you work with the credit bureaus and other key agencies to restore your good name.

We also recognize that people never really expect this sort of thing to happen to them, and you are probably wondering what you should do now. For that reason, we have prepared this Help Kit.

In the "What To Do Now" section of this kit, we provide you with:

- The names and contact information for key agencies, including the major credit bureaus
- Other important contacts you may need to make (with investment and credit card companies, the Department of Motor Vehicles, etc.)
- A checklist to help you keep track of the contacts you've made
- Samples of letters you will likely need to send to the credit bureaus and credit card companies to begin the process of disputing charges or accounts

In addition, we share some information with you about how identity theft can occur, since at this point you may not know how someone may have stolen your identity. Unfortunately, there are many ways that identity thieves can obtain your personal information and we've outlined some of the more common ways in the section "How Identity Theft Can Occur."

Finally, because you will want to protect yourself as much as you can in the future, we've included some tips on protecting your personal information in the section titled "What To Do Going Forward."

We hope that the information provided in this kit will be helpful to you. And, of course, your Chase representative is here to help you through this process.

What To Do *Now*

Now that you suspect that someone may have stolen your identity, you have already taken the first important step of contacting your Chase customer service representative. Chase will work with you every step of the way to resolve your situation at Chase. Below we have outlined additional steps that you can take to help restore your good name. Please note: You may want to use the **Action Taken Form** on page 6 to document the steps you've taken.

Chase

1. There may be some additional information that your Chase representative needs in order to help you. Please review the letter that you received with this kit carefully. If you have any questions, please call the number that is included in the letter you received with this kit.

Key Agencies to Contact

You will probably want to start by contacting the major credit bureaus, your local police department and the Federal Trade Commission. The contact information for each is below.

1. Start by contacting the fraud departments of each of the three major credit bureaus. The credit bureaus maintain reports that track the credit accounts that have been opened in your name and how you pay your bills. You should call first and then follow up in writing (see sample letter on page 7.)

Equifax		Experian		TransUnion	
Call	1-800-525-6285	Call	1-888-397-3742	Call	1-800-680-7289
Write:	P.O. Box 740241 Atlanta, Georgia 30374-0241	Write:	P. O. Box 949 Allen, Texas 75013-0949	Write:	Fraud Victim Assistance Division P.O. Box 6790 Fullerton, CA 92634
	www.equifax.com		www.experian.com		www.tuc.com

With each bureau you contact, take the following steps:

a. Request that a "fraud alert" be placed in your file.

b. Request a victim's statement asking that creditors call you before opening any new accounts or changing your existing accounts.

c. Ask for copies of your credit reports. Credit bureaus must give you a free copy of your report if your report is inaccurate because of fraud.

- Review the report carefully to make sure that no **additional fraudulent accounts** have been opened or unauthorized changes made.
- Check the inquiry section of the report. When **"inquiries"** appear from companies that opened fraudulent accounts, request the "inquiries" be removed from your report.
- In a few months, order a new copy of your credit report to verify your corrections and changes.
- After reviewing your credit report, you may find that accounts were opened in your name at other banks or lenders. Call the company where the account was opened to

report fraudulent accounts, then follow up in writing. Include copies (not originals) of documents that support your position. A sample dispute letter can be found on page 7.

2. File a report with your **local police** or the police in the community where the identity theft took place. Even if the police are unable to catch the thief, having a copy of the police report can help you in dealing with creditors.

   - Obtain a copy of the Police Report in case your bank, credit card company or others need proof of the crime.

3. Contact the **Federal Trade Commission's Identity Theft Hotline** at 1-877-IDTHEFT (1-877-438-4338). The FTC will put your information into a secure consumer fraud database and may, in appropriate instances, share it with other law enforcement agencies.

Other Important Contacts

You will probably want to take several additional steps to ensure that your accounts are secure. You should review transactions on credit account statements (including credit cards, home equity loans, etc.), bank accounts, investment accounts, and telephone. If you suspect that an identity thief may have tampered with any of these accounts, key contact information is detailed below.

TIP: Check your mail carefully.

- If you receive statements for accounts you do not have, contact the creditor. An identity thief may have opened an account in your name.
- If you do not receive statements from any of your usual accounts (including credit, banking and investment), contact the company immediately. An identity thief may have submitted a change of address in order to redirect your statements to a different location.
- If you do not receive any mail, contact the post office. An identity thief may have falsified a change of address to redirect your mail to a different location.

1. **Credit -** Contact **creditors,** which can include credit card, phone and other utility companies and banks and other lenders.

   If an identity thief has tampered with an existing account or opened an account fraudulently:

   - Ask to speak with someone in the company's security or fraud department and follow up with a letter. NOTE: It is important to notify credit card companies in writing as that is the consumer protection procedure the law (Fair Credit Billing Act) spells out for resolving errors on credit card billing statements. A sample dispute letter can be found on page 8.
   - Close accounts that have been tampered with and open new ones with new Personal Identification Numbers (PINs) and passwords.

   If an identity thief has changed the billing address on an existing credit card account*:*

   - Close the account.
   - When you open a new account, ask that a password be used before any inquiries or changes be made. Avoid using easily available information for a password like a date of birth, Social Security number, etc.

2. **Bank Accounts –** If an identity thief has tampered with your savings or checking account or ATM card, close the account immediately. Open a new account and ask that a password be used to obtain any information (and avoid using easily available information, e.g., your birth date, for a password.) If your checks were stolen or misused, either place a stop payment on the range of missing checks or close the account. Also, contact the major check verification companies to request that they notify retailers using their database.

TeleCheck:	1-800-710-9898
International Check Services:	1-800-631-9656
Equifax:	1-800-437-5120

3. **Investments -** If an identity thief has tampered with your securities, investments or brokerage account, immediately report it to your broker or account manager and to the Securities and Exchange Commission.

4. **Telephone Service –** If an identity thief has established a new phone service (including cellular) in your name and is making unauthorized calls, contact your service provider immediately to cancel the account. If you have trouble getting fraudulent phone charges removed from your account, contact your state Public Utilities Commission for local service or the Federal Communications Commission for long distance service providers.

5. **Stolen Mail –** If an identity thief has stolen your mail to obtain credit or falsified change of address forms, that's a crime. Report it to your local postal inspector. You can learn how to contact your local postal inspection service office by contacting your local post office or by visiting the United States Postal Service online at www.usps.gov/websites/depart/inspect.

6. **Employment –** If you believe someone is using your Social Security number to apply for a job or to work, contact the Social Security Fraud Hotline at 1-800-269-0271. You can also contact the Social Security Department at 1-800-772-1213 to verify the accuracy of the earnings reported on your Social Security number and to request a copy of your Social Security statement.

7. **Driver's License –** If you suspect your name is being used by an identity thief to get a driver's license or ID card, contact your Department of Motor Vehicles.

ACTION TAKEN

Use this form to record the steps you've taken to report the fraudulent use of your identity.

Credit Bureaus – Report Fraud

Bureau	Phone Number	Date Contacted	Contact Person	Comments
Equifax	1-800-525-6285			
Experian	1-888-397-3742			
TransUnion	1-800-680-7289			

Banks, Investment Companies, Credit Card Issuers and Other Creditors (Contact each creditor promptly to protect your legal rights)

Bank/Investment/Creditor	Address & Phone Number	Date Contacted	Contact Person	Comments

Law Enforcement Authorities – Report Identity Theft

Agency/Dept.	Phone Number	Date Contacted	Contact Person	Report Number	Comments
Federal Trade Commission	1-877-438-4338				
Local Police Department					

Sample dispute letter - Credit Bureau

Date

Your Name
Your Address
Your City, State, Zip

Complaint Department
Name of Credit Bureau
Address
City, State, Zip

Dear Sir or Madam:

I am writing to dispute the following information in my file. The items I dispute are circled on the attached copy of the report I received. ***(Identity item(s) disputed by name of source, such as creditors or tax court, and identify type of item, such as credit account, judgment, etc.)***

This item is ***(inaccurate or incomplete)*** because ***(describe what is inaccurate or incomplete and why)***. I am requesting that the item be deleted ***(or request another specific change)*** to correct the information.

Enclosed are copies of ***(use this sentence if applicable and describe any enclosed documentation, such as payment records, court documents)*** supporting my position. Please investigate this ***(these)*** matter***(s)*** and ***(delete or correct)*** the disputed item***(s)*** as soon as possible.

Sincerely,

Your Name

Enclosures: ***(List what you are enclosing)***

Sample dispute letter – Credit Card Issuers

Date

Your Name
Your Address
Your City, State, Zip
Your account number

Name of Creditor
Billing Inquiries
Address
City, State, Zip

Dear Sir or Madam:

I am writing to dispute a billing error in the amount of $_____ on my account. The amount is inaccurate because ***(describe the problem)***. I am requesting that the error be corrected, that any finance or other charges related to the disputed amount be credited as well, and that I receive an accurate statement.

Enclosed are copies of ***(use this sentence to describe any enclosed information, such as sales slips, payment records)*** supporting my position. Please investigate this matter and correct the billing error as soon as possible.

Sincerely,

Your Name

Enclosures: ***(List what you are enclosing)***

How Identity Theft Can Occur

Despite your best efforts to manage the flow of your personal information or keep it to yourself, skilled identity thieves may use a variety of methods (both low and high tech) to gain access to your data.

How do identity thieves get your personal information? They:

- Steal wallets and purses containing your identification, credit and bank cards.
- Steal your mail, including your bank and credit card statements, pre-approved credit offers, telephone calling cards and tax information.
- Complete a "change of address form" to divert your mail to another location.
- Rummage through your trash, or the trash of businesses, for personal data in a practice known as "dumpster diving."
- Fraudulently obtain your credit report by posing as a landlord, employer or someone else who may have a legitimate need for – and a legal right to – the information.
- Get your business or personal records at work.
- Find personal information in your home.
- Use personal information you share on the Internet.
- Buy your personal information from "inside" sources. For example, an identity thief may pay a company employee for information about you that appears on an application for goods, services or credit.

How do identity thieves use your personal information? They:

- Call your credit card issuer and, pretending to be you, ask to change the mailing address on your credit card account. The imposter then runs up charges on your account. Because your bills are being sent to the new address, it may take some time before you realize there's a problem.
- Open a new credit card account using your name, date of birth and Social Security number. When they use the credit card and don't pay the bills, the delinquent account is reported on your credit report.
- Establish phone or wireless service in your name.
- Open a bank account in your name and write bad checks on that account.
- File for bankruptcy under your name to avoid paying debts they've incurred in your name or to avoid eviction.
- Use counterfeit checks or debit cards and drain your bank account.
- Buy cars by taking out auto loans in your name.

In the next section, we describe some steps you can take going forward to protect your personal information from identity thieves.

What To Do Going Forward

Identity theft and account fraud are serious issues. And, at Chase, we believe the more you understand how they can occur, the better you'll be able to take precautions to protect yourself. Chase works hard every day to ward off these threats, but even tighter security is possible only with your help. You may be aware of many of the steps you can take to stop these crimes before they happen, but some tips may be new to you. For that reason, we have outlined some steps you can take to prevent someone from stealing your identity in the future. While nothing is foolproof, following the steps outlined below can help to protect you.

1. Carry only what you need. The less personal information you have with you the better off you will be if you have your purse or wallet stolen.

2. Don't put outgoing mail in or on your mailbox. Drop it into a secure, official Postal Service collection box. Thieves may use your mail to steal your identity. Consider a home shredder for all sensitive documents.

3. Cancel any credit card accounts that you no longer use.

4. Don't pre-print your driver's license, telephone or Social Security numbers on your checks.

5. Report lost or stolen checks immediately. Chase will block payment on the check numbers involved. Also, review new checks to make sure none have been stolen in transit.

6. Store cancelled checks—and new checks—in a safe place.

7. Notify Chase of suspicious phone inquiries such as those asking for account information to "verify a statement" or "award a prize."

8. You should guard your ATM and credit card receipts. Thieves can use them to access your accounts. Never throwaway receipts in a public trash can.

9. Guard your Personal Identification Numbers (PINs) for your ATM and credit cards, and don't write on or keep your PINs with your cards.

10. If you receive financial solicitations that you're not interested in, tear them up before throwing them away, so thieves can't use them to assume your identity. Destroy any other financial documents, such as bank statements or invoices, before disposing of them.

11. Don't give out financial information such as checking account and credit card numbers—and especially your Social Security number—on the phone unless you initiate the call and know the person or organization you're dealing with. Don't give that information to any stranger, even one claiming to be from Chase.

12. If regular bills fail to reach you, call the company to find out why. Someone may have filed a false change-of-address notice to divert your information to his or her address.

13. If your bills include suspicious items, don't ignore them. Instead, investigate immediately to head off any possible fraud before it occurs.

14. Periodically contact the major credit reporting companies to review your file and make certain the information is correct. For a small fee, you can obtain a copy of your credit report at any time. The three major credit bureaus are:

Equifax	1 (800) 685-1111
Experian	1 (800) 682-7654

TransUnion 1 (800) 916-8800

15. Chase is committed to ensuring the privacy of your online transactions through the latest security technology. That's why for Internet-based communications we require the use of a browser that supports 128-bit encryption for the new, Internet-based product, Chase Online™. 128-bit encryption is the highest level of data protection that is commonly available in today's Internet browsers and is needed to provide the approximate level of security we provide for our non-Internet based online banking products, such as Chase Online Banking, which uses a dial-up or "virtual private network" approach to transmission security.

    Another online safety feature is your password. Every time you log on to Chase Online™, you are required to enter your ID and password. You control both and can change your password at any time. For your safety, you should not reveal your password to anyone. For more information about how you are protected when using Chase Online™, or for more information about encryption, visit us at Chase.com.

Together, you and Chase may be able to head off identity theft and account fraud before they ever happen. If you would like more information about identity theft, you can visit the Federal Trade Commission's (FTC) consumer website at www.consumer.gov/idtheft, or you can call the FTC toll-free at (1-877) IDTHEFT (438-4338).

CHASE

THE RIGHT RELATIONSHIP IS EVERYTHING.®

Authorization to Disclose Information

I, the undersigned, do give to Chase Manhattan Corporation, The Chase Manhattan Bank, Chase Manhattan Bank USA, National Association and any of their direct or indirect subsidiaries ("Chase") authorization to discuss and disclose with third parties the details concerning my claim of fraudulent establishment and/or use of account(s) in my name with Chase. This authorization is in addition to any other instruction that I may have already provided concerning Chase sharing information about me with any third parties. If there is a conflict between this authorization and any previous instructions, this authorization will control.

I understand Chase will respond to requests for information concerning my claim, but not initiate any calls on my behalf. By Chase honoring this authorization, I agree to indemnify and hold Chase harmless from any and all claims, losses or other costs or expenses which Chase may incur as a result of its reliance on this authorization. This action in no way obligates Chase nor makes Chase a party to any action with respect to my claim upon a third party. Any actions by Chase will be considered on a best effort basis in assisting me in resolving my claim with a third party(ies).

Name:_____

Address:_____

Reference Number:_____

Signature:_____

Date:_____