US00RE43845E

(19) **United States**

(12) **Reissued Patent**

Rothfarb

(10) **Patent Number: US RE43,845 E**

(45) **Date of Reissued Patent: Dec. 4, 2012**

(54) **LOCK-AND-KEY CONSUMER BILLING DATA PROTECTION SYSTEM HAVING DATA ENCRYPTION CAPABILITY**

(75) Inventor: **Neil Barry Rothfarb**, West Hartford, CT (US)

(73) Assignee: **Nebarb Software Foundation L.L.C.**, Wilmington, DE (US)

(21) Appl. No.: **12/118,663**

(22) Filed: **May 9, 2008**

Related U.S. Patent Documents

Reissue of:

(64) Patent No.: **7,043,452**
Issued: **May 9, 2006**
Appl. No.: **10/160,765**
Filed: **May 31, 2002**

U.S. Applications:

(63) Continuation-in-part of application No. 10/146,252, filed on May 15, 2002, and a continuation-in-part of application No. 10/146,249, filed on May 15, 2002.

(51) **Int. Cl.**
G06F 21/00 (2006.01)

(52) **U.S. Cl.** **705/50**; 705/2; 705/51; 705/77; 705/40; 380/203; 713/165; 713/200

(58) **Field of Classification Search** 705/40, 705/50

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,123,747	A		10/1978	Lancto
5,432,851	A		7/1995	Scheidt
5,455,953	A		10/1995	Russell
5,590,197	A		12/1996	Chen
5,706,442	A		1/1998	Anderson
5,727,163	A		3/1998	Bezos
5,745,556	A	*	4/1998	Ronen 379/127.05
5,748,718	A		5/1998	Manicone
5,960,411	A	*	9/1999	Hartman et al. 705/26
6,128,603	A		10/2000	Dent
6,408,284	B1		6/2002	Hilt
6,676,016	B1		1/2004	Coskrey, IV
6,839,687	B1		1/2005	Dent

(Continued)

FOREIGN PATENT DOCUMENTS

JP	363316626	A	12/1988

OTHER PUBLICATIONS

"The Bank Credit Card Business," 2d ed., American Bankers Association, Washington, D.C., 1996, 243 pages.

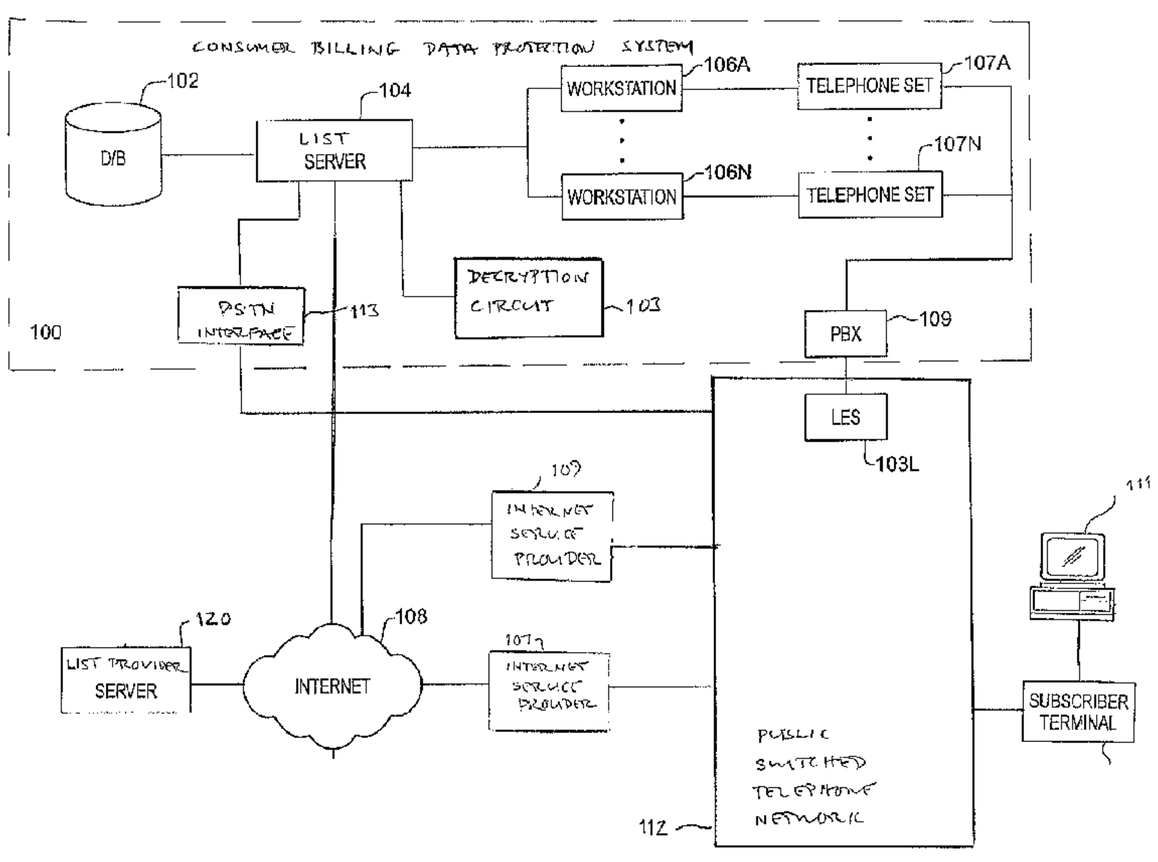
(Continued)

Primary Examiner — Jacob C. Coppola

(57) **ABSTRACT**

A "lock-and-key" consumer billing data protection capability is provided to telemarketing and electronic marketing systems which are based upon previously-acquired consumer lists. The lists contain encrypted partial billing information for each consumer, which is insufficient to access the consumer's account. Thus, at the time a consumer is offered a product or service, the telemarketer, the electronic marketer, and any entity hired to perform billing operations for such consumer purchases all remain "locked" out from accessing the consumer's account. When the consumer wishes to authorize the purchase of an offered product or service, the consumer must provide the "key" to the consumer's account, which is the key necessary to decrypt the encrypted partial billing information and also the missing billing information not acquired from the list provider.

33 Claims, 3 Drawing Sheets



U.S. PATENT DOCUMENTS

6,868,403	B1	3/2005	Wiser	
7,043,452	B2	5/2006	Rothfarb	
2002/0184089	A1	12/2002	Tsou	
2003/0187788	A1	10/2003	Rothfarb	
2003/0216980	A1	11/2003	Rothfarb	
2003/0216999	A1	11/2003	Rothfarb	
2005/0065883	A1	3/2005	Dent	
2005/0080736	A1	4/2005	Dent	
2006/0129835	A1 *	6/2006	Ellmore	713/183
2007/0005427	A1	1/2007	Walker	
2008/0147564	A1	6/2008	Singhal	

OTHER PUBLICATIONS

"Borland® Paradox® for Windows: User's Guide," Version 5.0, Borland International, Inc., Scotts Valley, Calif., 1994, 188 pages.
Bragg, S. M., "Accounting Best Practices," Wiley, New York, 1999, 290 pages.
Chopra, S., and P. Meindl, "Supply Chain Management: Strategy, Planning, and Operation," Prentice-Hall, Upper Saddle River, N.J., 2001, 459 pages.
Danish, S., and P. Gannon, "Building Database-Driven Web Catalogs," McGraw-Hill, New York, 1998, 263 pages.
Derfler, Jr., F. J., and L. Freed, "How Networks Work," Millennium Edition, Que Corporation, Indianapolis, Sep. 2000, 230 pages.
Dobler, D. W., and D. N. Burt, "Purchasing and Supply Management: Text and Cases," 6th ed., McGraw-Hill, New York, 1996, 806 pages.
"Federal Trade Commission, 16 CFR Part 310, Telemarketing Sales Rule, Proposed Rules," Federal Register, Part II, vol. 67, No. 20, Jan. 30, 2002, pp. 4492-4546.
Gavron, J., and J. Moran, "How to Use Microsoft Windows NT 4 Workstation," Macmillan Computer Publishing, Emeryville, Calif., 1996, 198 pages.
Gralla, P., "How the Internet Works," 6th ed., Que Corporation, Indianapolis, Sep. 7, 2001, 354 pages.
Muller, N. J., "Desktop Encyclopedia of the Internet," Artech House, Norwood, Mass., Nov. 1998, 566 pages.
"Restatement of the Law, Second (Student Edition): Contracts 2d, Pamphlet 1 §§ 1-177, With Reporter's Notes," American Law Institute, St. Paul, Minn., 1981, pp. I-XXIV, 1-243.
Riley, D. D., "Data Abstraction and Structures: An Introduction to Computer Science II," Boyd & Fraser Publishing, Boston, 1987, pp. v-xviii, 1-3, 653-662.
White, J. J., and R. S. Summers, "Uniform Commercial Code," 4th ed., West Publishing Co., St. Paul, Minn., 1995, pp. xxv-xxix, 1019-1043.
White, R., "How Computers Work," Millennium Edition, Que Corporation, Indianapolis, Sep. 1999, 284 pages.
Office Action dated Apr. 27, 2007, from U.S. Appl. No. 10/107,863, filed Mar. 26, 2002.
Final Office Action dated Jan. 10, 2008, from U.S. Appl. No. 10/107,863, filed Mar. 26, 2002.
Office Action dated Jul. 31, 2008, from U.S. Appl. No. 10/107,863, filed Mar. 26, 2002.
Office Action dated Jan. 31, 2006, from U.S. Appl. No. 10/146,249, filed May 15, 2002.
Final Office Action dated Jul. 19, 2006, from U.S. Appl. No. 10/146,249, filed May 15, 2002.
Board of Appeals Decision dated Sep. 22, 2008, from U.S. Appl. No. 10/146,249, filed May 15, 2002.
Restriction Requirement dated Aug. 23, 2007, from U.S. Appl. No. 10/146,252, filed May 15, 2002.
Office Action dated Dec. 13, 2007, from U.S. Appl. No. 10/146,252, filed May 15, 2002.
Final Office Action dated Jun. 27, 2008, from U.S. Appl. No. 10/146,252, filed May 15, 2002.
Office Action dated Apr. 6, 2005, from U.S. Appl. No. 10/160,765, filed May 31, 2002, now U.S. Patent No. 7,043,452, which is a Continuation-in-Part of the present application.
Notice of Allowance dated Dec. 7, 2005, from U.S. Appl. No. 10/160,765, filed May 31, 2002, now U.S. Patent No. 7,043,452, which is a Continuation-in-Part of the present application.
Restriction Requirement dated Sep. 19, 2005, from U.S. Appl. No. 10/146,249, filed May 15, 2002.
Final Office Action dated Mar. 3, 2009, from U.S. Appl. No. 10/107,863, filed Mar. 26, 2002.
Examiner's Interview Summary dated Jun. 11, 2009, from U.S. Appl. No. 10/107,863, filed Mar. 26, 2002.
Advisory Action dated Jul. 2, 2009, from U.S. Appl. No. 10/107,863, filed Mar. 26, 2002.
Notice of Panel Decision From Pre-Appeal Brief Review dated Aug. 20, 2009, from U.S. Appl. No. 10/107,863, filed Mar. 26, 2002.
Examiner's Answer to Appeal Brief, dated Oct. 15, 2009, from U.S. Appl. No. 10/107,863, filed Mar. 26, 2002.

* cited by examiner

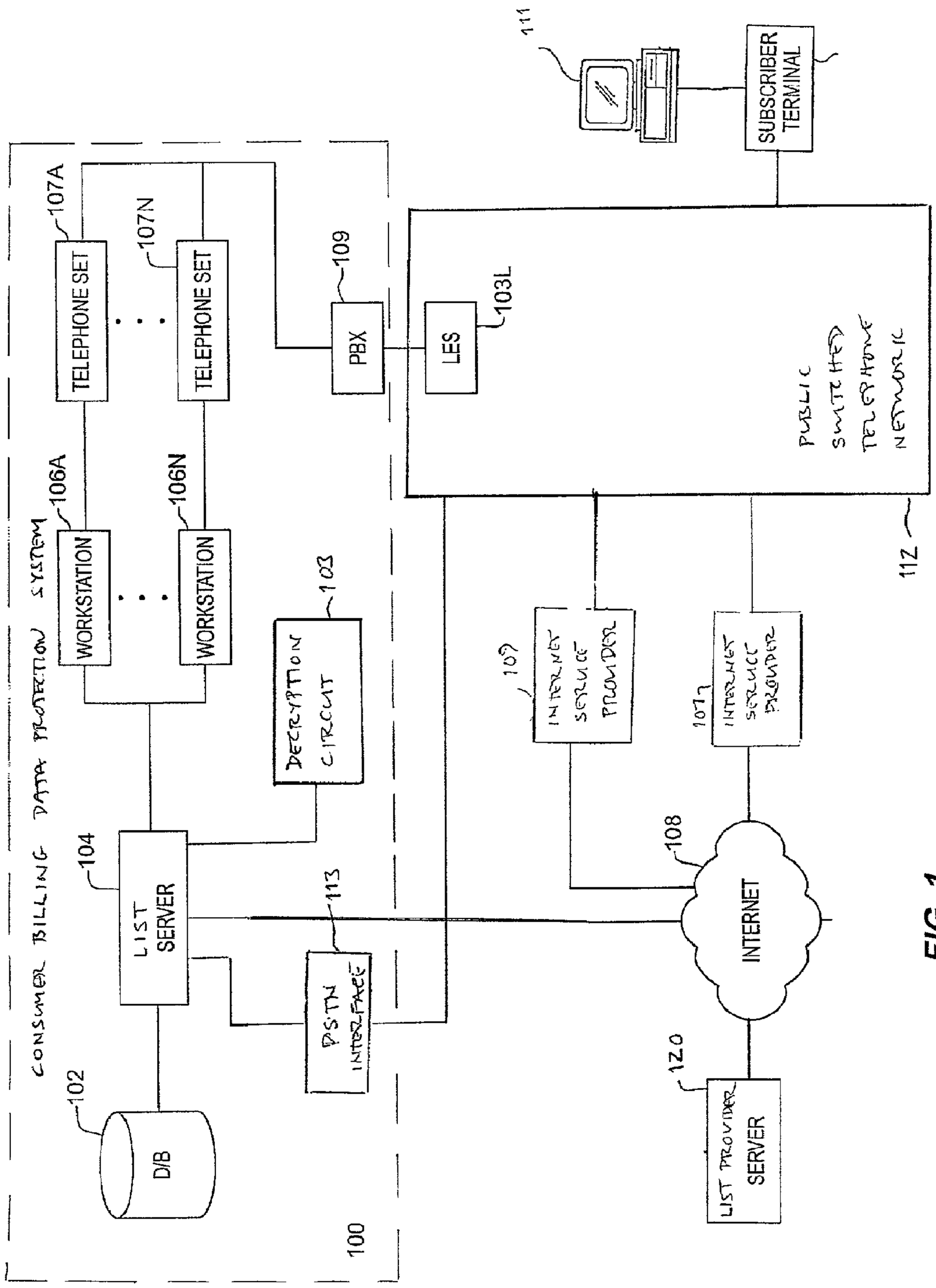

CONSUMER BILLING DATA PROTECTION SYSTEM
100
111
SUBSCRIBER TERMINAL
107A
107N
TELEPHONE SET
TELEPHONE SET
106A
106N
WORKSTATION
WORKSTATION
104
LIST SERVER
102
D/B
DECRYPTION CIRCUIT
103
113
PSTN INTERFACE
109
PBX
LES
103L
PUBLIC SWITCHED TELEPHONE NETWORK
112
107
INTERNET SERVICE PROVIDER
107
INTERNET SERVICE PROVIDER
108
INTERNET
120
LIST PROVIDER SERVER

FIG. 1

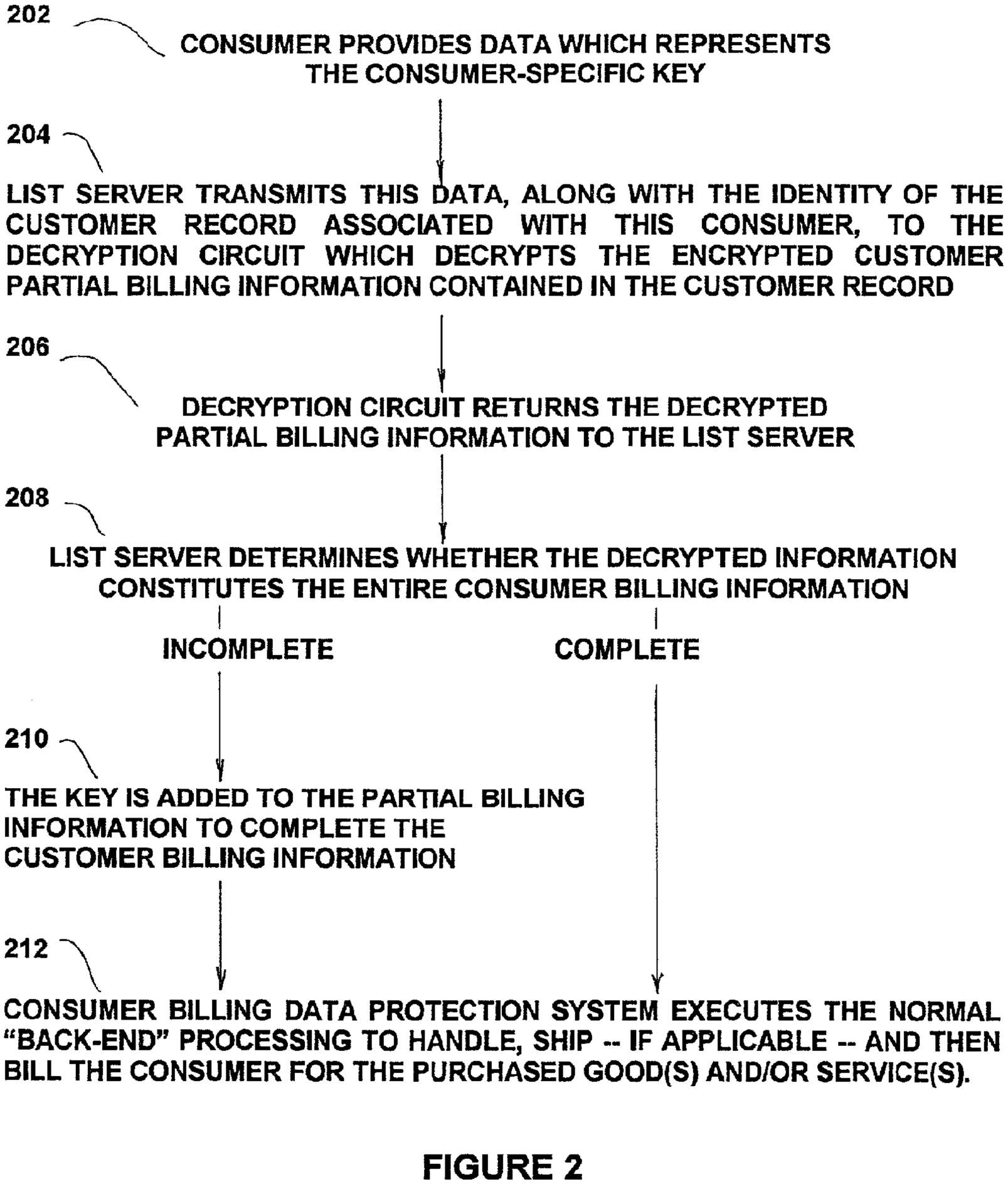

202
CONSUMER PROVIDES DATA WHICH REPRESENTS THE CONSUMER-SPECIFIC KEY
204
LIST SERVER TRANSMITS THIS DATA, ALONG WITH THE IDENTITY OF THE CUSTOMER RECORD ASSOCIATED WITH THIS CONSUMER, TO THE DECRYPTION CIRCUIT WHICH DECRYPTS THE ENCRYPTED CUSTOMER PARTIAL BILLING INFORMATION CONTAINED IN THE CUSTOMER RECORD
206
DECRYPTION CIRCUIT RETURNS THE DECRYPTED PARTIAL BILLING INFORMATION TO THE LIST SERVER
208
LIST SERVER DETERMINES WHETHER THE DECRYPTED INFORMATION CONSTITUTES THE ENTIRE CONSUMER BILLING INFORMATION
INCOMPLETE
COMPLETE
210
THE KEY IS ADDED TO THE PARTIAL BILLING INFORMATION TO COMPLETE THE CUSTOMER BILLING INFORMATION
212
CONSUMER BILLING DATA PROTECTION SYSTEM EXECUTES THE NORMAL "BACK-END" PROCESSING TO HANDLE, SHIP -- IF APPLICABLE -- AND THEN BILL THE CONSUMER FOR THE PURCHASED GOOD(S) AND/OR SERVICE(S).

FIGURE 2

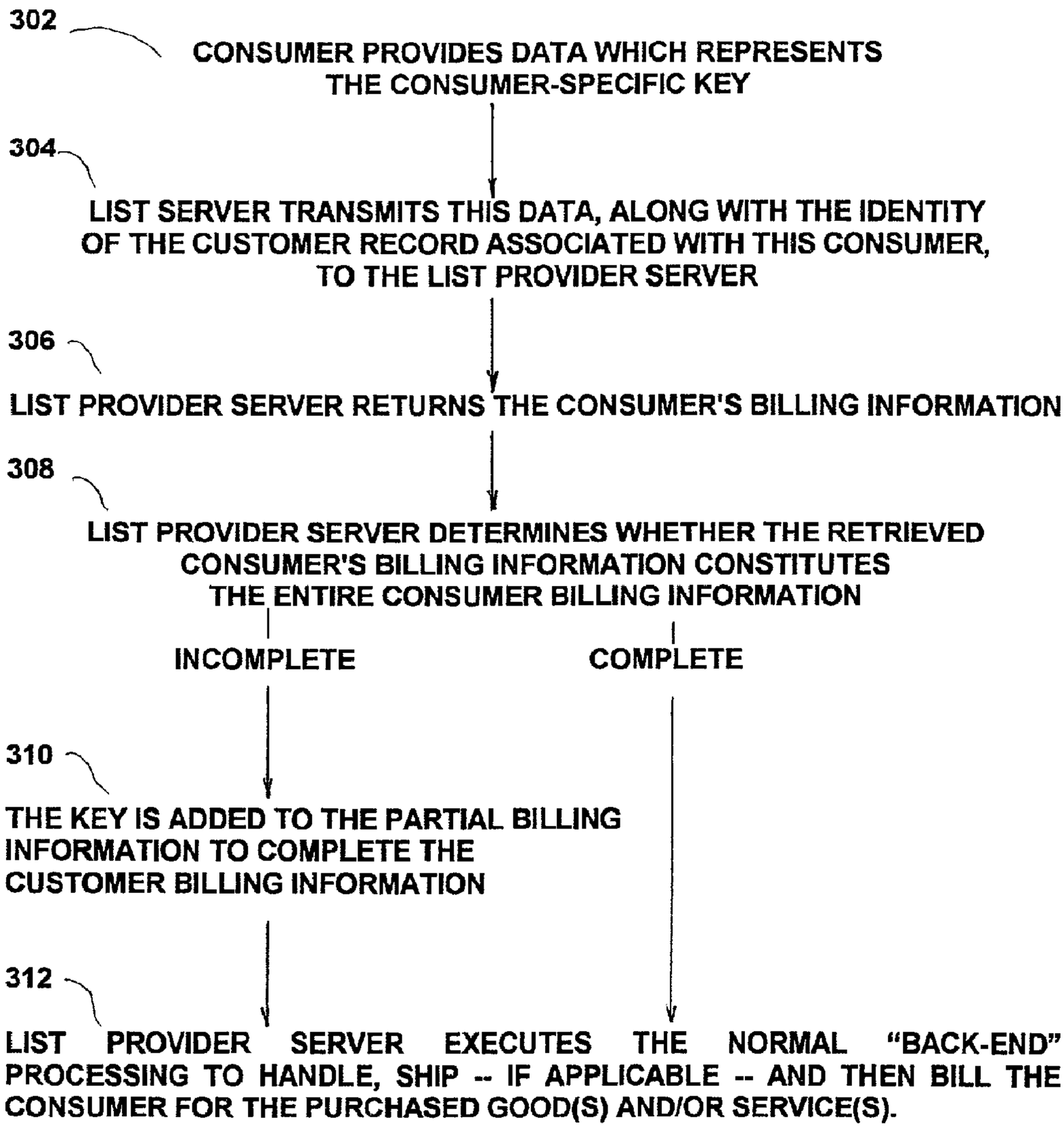

302
CONSUMER PROVIDES DATA WHICH REPRESENTS THE CONSUMER-SPECIFIC KEY
304
LIST SERVER TRANSMITS THIS DATA, ALONG WITH THE IDENTITY OF THE CUSTOMER RECORD ASSOCIATED WITH THIS CONSUMER, TO THE LIST PROVIDER SERVER
306
LIST PROVIDER SERVER RETURNS THE CONSUMER'S BILLING INFORMATION
308
LIST PROVIDER SERVER DETERMINES WHETHER THE RETRIEVED CONSUMER'S BILLING INFORMATION CONSTITUTES THE ENTIRE CONSUMER BILLING INFORMATION
INCOMPLETE
COMPLETE
310
THE KEY IS ADDED TO THE PARTIAL BILLING INFORMATION TO COMPLETE THE CUSTOMER BILLING INFORMATION
312
LIST PROVIDER SERVER EXECUTES THE NORMAL "BACK-END" PROCESSING TO HANDLE, SHIP -- IF APPLICABLE -- AND THEN BILL THE CONSUMER FOR THE PURCHASED GOOD(S) AND/OR SERVICE(S).

FIGURE 3

LOCK-AND-KEY CONSUMER BILLING DATA PROTECTION SYSTEM HAVING DATA ENCRYPTION CAPABILITY

Matter enclosed in heavy brackets [ ] appears in the original patent but forms no part of this reissue specification; matter printed in italics indicates the additions made by reissue.

CROSS REFERENCE TO RELATED APPLICATIONS

This application is a continuation in part of, and claims priority to, U.S. patent application Ser. No. 10/146,249, titled "Lock-And-Key Consumer Billing Data Protection For Electronic Marketing" and U.S. patent application Ser. No. 10/146,252 titled "Lock-And-Key Consumer Billing Data Protection For Telemarketing", both of which are filed on May 15, 2002, which are hereby incorporated by reference in their entirety.

FIELD OF THE INVENTION

The present invention relates generally to computer systems, and more particularly to computerized order entry systems that support and facilitate telemarketing and consumer electronic marketing operations.

Problem

The practice of companies offering to sell goods or services to consumers directly over the telephone, without requiring the consumer to visit a traditional ("bricks and mortar") store, is known as telemarketing. In today's business climate, telemarketing has become ubiquitous.

Historically, one of the primary problems with telemarketing was that telemarketers did not precisely target consumers who were likely to buy their products or services. Rather, telemarketers routinely employed "cold calls" in an attempt to reach a broad range of consumers. Recently, however, telemarketers have recognized that consumers and the companies providing the goods and services which they market and sell would all benefit from targeted telemarketing. Accordingly, telemarketers have begun to target their efforts to those consumers who most likely would be receptive to the specific products and/or services being offered. Specifically, a telemarketing company attempting to sell a product or service of one of its clients may acquire from a third-party a list of consumers who recently purchased other products or services. For example, a telemarketing company attempting to sell memberships in a dial-in roadside assistance service program may acquire a recent consumer list from a third-party vendor of car telephones.

In an analogous manner, direct marketers have begun to acquire lists of consumers for targeted electronic messages that contain product and/or service solicitations. For example, marketers contact consumers on-line over the Internet via electronic mail, instant messaging and the like. They are also employed in other electronic marketing systems in which, for example, marketers contact consumers with messages on their mobile phones, personal data assistants (PDAs) and the like via various wireless communications protocols.

When a consumer agrees to purchase a product or service offered by a marketer or telemarketer, in order to access that consumer's account (i.e., bill that consumer), it is necessary to possess certain "billing information." At a minimum, this billing information includes the entire number, typically sixteen digits, of the consumer's credit card. The same billing information is required regardless of whether the entity accessing the consumer's account is the marketer/telemarketer itself, the seller, or any other entity hired to perform the billing operations.

There are two general approaches presently employed to acquire this billing information necessary to access a consumer's account.

The first approach is to acquire all of a consumer's billing information from the list provider that provided the consumer list. Under this approach, a consumer's billing information is often acquired from the list provider before the consumer is contacted. Variations on this approach include acquiring a consumer's billing information only after the consumer is contacted and indicates that they want to purchase the offered product or service with the same credit used for the prior purchase (commonly referred to as a "matchback"). Under the variations of this approach, however, all of the consumer's billing information is ultimately acquired from the list provider—consumers do not need to provide any billing information themselves.

Presently, list providers sometimes transfer encrypted complete billing information to telemarketers, electronic marketers, or companies hired to perform their payment operations. This encrypted complete billing information can be decrypted only by using a cipher key provided by the list provider. Importantly, the list provider releases this cipher key without the consumer providing the telemarketer or electronic marketer any authorization or per transaction-based "key." Thus, the consumer's account can be charged even if the consumer does not reach into their wallet to provide a "key" or any other billing information.

The advantage of this approach is that it eliminates the need for consumers to transmit their credit card number. This protects consumers from transmitting billing information sufficient to access their account.

The disadvantage of this approach, however, is that consumers are not in control of their billing information. As long as a marketing/telemarketing company professes to have interpreted some response from a consumer as authorizing a purchase, the consumer's account can be charged.

The second approach is to acquire all of a consumer's billing information directly from the consumer. If a consumer wants to accept an offer to purchase a product or service, that consumer must then provide their entire credit card number to authorize the sale.

The advantage of this approach is that consumers are in control of their billing information. Without a consumer's credit card number, the consumer cannot be billed for goods and services.

The disadvantage of this approach, however, is that consumers must transmit all of their billing information. Consequently, consumers may transmit billing information sufficient to access their account to untrustworthy sales agents employed by legitimate telemarketers and/or entities that are not legitimate marketers/telemarketers. In addition, this approach produces billing mistakes due to errors in the transmission and communication of the consumers' billing information.

Therefore, given the above, what is needed is a lock-and-key consumer billing data protection capability that combines some or all of the advantages of the above-described approaches, while eliminating or reducing some or all of their respective disadvantages.

Solution

The present lock-and-key consumer billing data protection system having data encryption capability provides customer

billing account security to marketing and telemarketing systems which operate using consumer lists that may be acquired from a list provider.

The lock-and-key consumer billing data protection system having data encryption capability, in one embodiment, includes a database that stores consumer records presently available to the marketer/telemarketer or acquired from a list provider, such as third-parties from whom such consumers have previously purchased goods or services. Each stored consumer record includes consumer identification information and partial billing information. The partial billing information (fewer than all of the alphanumeric characters needed to access a consumer's account) in each consumer account is encrypted, using a consumer-specific cipher key, such that the marketer/telemarketer, seller and companies hired to perform billing operations are "locked" out of every consumer's account unless they receive the decryption key from the consumer. In order to provide a simple decryption process, that does not require the previous exchange of a negotiated set of keys between the consumer and the marketer/telemarketer, a predetermined set of digits from the consumer's account is used as the key to decrypt the partial billing information stored in the database as well as to provide the missing billing information not yet stored in the database. In the case where the entirety of the consumer's billing information is encrypted, the consumer provided key is used to decrypt the consumer's billing information.

Therefore, if a consumer wishes to purchase a product or service being offered, the consumer must provide the "key" to decrypt the partial billing information stored in the consumer's account, which key is also the missing billing information not yet stored in the database. Only after the consumer supplies the "key," can the consumer be charged. Specifically, now that all the consumer's billing information has been acquired—partly from the list provider and partly from the consumer—can the consumer's account can be accessed by the marketer/telemarketer, seller or an entity hired to perform billing operations for such purchases.

One advantage of the lock-and-key consumer billing data protection system having data encryption capability is that consumers are in control of their billing information. Without receiving the missing billing information (the "key") from the consumer, no entity can bill the consumer based on an erroneous premise that authorization for a particular transaction was received. Unlike the presently employed approach of acquiring all of a consumer's billing information from a third party, the lock-and-key consumer billing data protection system having data encryption capability "locks" companies out of a consumer's account until the consumer takes the proactive step of providing the missing billing information—the "key".

Further features and advantages of the invention as well as the structure and operation of various embodiments of the lock-and-key consumer billing data protection system having data encryption capability are described in detail below with reference to the accompanying drawings.

BRIEF DESCRIPTION OF THE FIGURES

The features and advantages of the present lock-and-key consumer billing data protection system will become more apparent from the detailed description set forth below when taken in conjunction with the drawings in which like reference numbers indicate identical or functionally similar elements. Additionally, the left-most digit of a reference number identifies the drawing in which the reference number first appears.

FIG. **1** is a block diagram illustrating the architecture of a lock-and-key consumer billing data protection system having data encryption capability and an environment in which it is operational;

FIGS. **2** and **3** are a flow charts depicting the operation of a lock-and-key consumer billing data protection system having data encryption capability.

DETAILED DESCRIPTION

Overview

The present lock-and-key consumer billing data protection system having data encryption capability relates to providing a "lock-and-key" consumer billing data protection capability to marketing and telemarketing systems. In an embodiment, a marketer/telemarketer selling particular good(s) and/or service(s) acquires a list of consumers (typically from a list provider) or has in its possession a list of consumers. This list typically identifies consumers who have previously purchased goods and/or services, thus allowing for targeted sales.

Such consumer lists presently available or transferred from the list provider contain only partial billing information (p alphanumeric characters of the m+p alphanumeric character consumer billing information) for each consumer. That is, the partial billing information comprises a predetermined subset of data from the consumer's complete billing data, and fails to include the entirety of the billing data. One such example is a string of consecutive digits of the consumer's account number. Because complete billing information is needed to access a consumer's account, the present lock-and-key consumer billing data protection system having data encryption capability "locks" out the marketer/telemarketer, the seller, and even an entity hired to perform billing operations for such purchases from accessing the consumer's account.

When a consumer takes a proactive step to unambiguously order the offered product(s) and/or service(s), the lock-and-key consumer billing data protection system having data encryption capability requires that they provide only certain numbers from their credit cards—the "key"—in order to authorize the purchase. This is done without allowing access to the consumer's partial billing information previously stored in the database system. The marketer/telemarketer, seller, or company hired to perform billing operations, however, now has all of the consumer's billing information and, as a result, can access that consumers account.

Lock-and-key consumer billing data protection empowers consumers with the ability to buy goods and services while controlling access to their account and eliminating the need to transmit all of their billing information. Thus, lock-and-key consumer billing data protection guards against consumers being billed for products or services whose purchase they did not, nor intend to, authorize by requiring consumers to take the affirmative, proactive step of communicating part of their billing information to authorize a purchase.

The consumer can directly contact the marketer/telemarketer to initiate an inbound communication session, or the telemarketer can contact the consumer to initiate an outbound communication session, and both cases can follow the sale of another product or service.

The present lock-and-key consumer billing data protection system having data encryption capability is described in terms of the above examples. This is for convenience only and is not intended to limit the application of the present lock-and-key consumer billing data protection system having data encryption capability. In fact, after reading the following description, it will be apparent to one skilled in the relevant

art(s) how to implement the lock-and-key consumer billing data protection system having data encryption capability in alternative embodiments.

Glossary

Below are definitions of terms used herein. In the event that a term defined herein has a more common meaning or usage, the definition provided herein should be taken as the intended meaning.

"Billing information" means the minimum data needed in order to charge or otherwise gain access to a consumer's account, such as a credit card, checking, savings, share or similar account, utility bill, mortgage loan account or debit card. In most instances, such minimum information is a set of alphanumeric characters, such as the typical sixteen-digit credit card account number.

"Credit card" means any debit, prepaid, charge, or credit card (whether private label or bank issued), or plate, coupon book or other credit device existing for the purpose of obtaining money, property, labor, or services as authorized by the consumer in whose name the credit card is issued.

"Consumer" means any person who is or may be required to pay for goods, services or a charitable contribution offered or solicited through telemarketing.

"Consumer identification information" means the data used to contact a consumer (e.g. name, telephone number, street address, electronic mail address, etc.).

"List Provider" means an entity that provides a list of consumers for use in sales activities. The list typically identifies consumers who recently purchased other products or services and typically includes only partial billing information (p alphanumeric characters of the m+p alphanumeric character consumer billing information) for each consumer, as noted above.

"Seller" means any person who provides, offers to provide, or arranges for others to provide goods or services to the consumer in exchange for consideration. For simplicity of description, the term "marketer/telemarketer" is used herein to include the instances where the marketer/telemarketer is also the seller, since such a distinction is unnecessary for the purpose of describing the operation of the lock-and-key consumer billing data protection system having data encryption capability.

"Marketer" means any person who, in connection with marketing activities (plans, programs or campaigns which are conducted to induce the purchase of goods or services or charitable contributions) initiates or receives electronic communications (electronic mail, instant or text messages and the like) to or from a consumer.

"Telemarketer" means any person who, in connection with telemarketing, initiates or receives telephone calls to or from a consumer. Further, the terms "user," "telemarketer," "telemarketing company," "entity," and the plural form of these terms are used interchangeably throughout herein to refer to those who would access, use, and/or benefit from the lock-and-key consumer billing data protection capability provided to telemarketing systems as described herein.

"Telemarketing" means a plan, program or campaign which is conducted to induce the purchase of goods or services or a charitable contribution, by use of one or more telephones.

Lock-and-Key System

FIG. **1** is a block diagram that illustrates the architecture of a lock-and-key consumer billing data protection system having data encryption capability **100**, termed "consumer billing data protection system" herein. FIG. **1** highlights the connectivity among the various data management components of the consumer billing data protection system **100** without providing all of the details of the typical apparatus that is specifically used to employ this system in either telemarketing or electronic marketing activities. The above-noted co-pending patent applications provide the details of such apparatus and also provide flow diagrams that illustrate the typical operation of these apparatus.

Consumer billing data protection system **100** includes a repository database **102**. Database **102**, in an embodiment, is a computer running database management server software with physical media which acts as a central store for information within consumer billing data protection system **100**. That is, database **102** stores the consumer lists presently available to the marketer/telemarketer or received from a list provider, including the consumer records containing consumers' identification information, the partial billing information, any key received from a consumer and possibly any collected demographic information. In an alternate embodiment, database **102** would only store records containing consumers' contact and demographic information. That is, a seller retains the partial billing information (except for the name of the credit card) for added consumer protection.

Returning to FIG. **1**, a list server **104** is the data processor of consumer billing data protection system **100**, and is connected to database **102**. List server **104** allocates, distributes and provides the data stored in database **102** to, in the telemarketing embodiment, a plurality of workstations **106** (shown in FIG. **1** as workstations **106**A-**106**N) used by a plurality of sales agents employed by a telemarketer. In this embodiment, list server **104** provides workstations **106** with graphical user interface (GUI) "front-end" screens to present certain data in the consumer records (one at a time) during the telemarketing process. In the electronic marketing embodiment, list server **104** retrieves certain data that is stored in database **102** and uses this data to originate electronic communications via electronic mail, instant messaging, text messages and the like to identified consumers in a well-known fashion.

Each of the plurality of sales agents is also equipped with a telephone station set **107** (shown in FIG. **1** as **107**A-**107**N) and the list server **104** is capable of originating outgoing telephone calls. Assuming for the purpose of the description herein that the sales agents are equipped with telephone station sets **107**, a Private Branch exchange (PBX) **109** functions to interconnect the telephone station sets **107** via trunks with a Local Exchange System (LES) **103**L. Local Exchange System **103**L is part of the Public Switched Telephone Network (PSTN) **112**. This allows the sales agents to originate calls to identified consumers in a well-known fashion.

Alternatively, the list server **104** can originate electronic messages for transmission to the consumers personal computer **111** via the Internet **108**. In this mode, the list server **104** generates an electronic message addressed to the consumer at their Internet e-mail address and transmits this message via a communications connection from list server **104** directly via the Internet **108** or to an Internet Service Provider **109** with whom the consumer billing data protection system **100** has an account. The Internet Service Provider **109** receives the electronic message and forwards the electronic message via the Internet **108** to the Internet Service Provider **107** with whom the consumer has an account. When the consumer connects to this Internet Service Provider **107** from their personal computer **111**, the Internet Service Provider **107** delivers the electronic message to the consumer. The consumer can have access to the Internet **108** in many ways, such as via the Public Switched Telephone Network **105**, cable modem, high speed data connection, satellite communications, and the like.

List server **104** also allows consumer billing data protection system **100** to store presently available consumer lists or

to receive the consumer lists from a list provider. That is, a plurality of servers, such as list provider server **120** belonging to list providers may be authorized to access consumer billing data protection system **100** via the public, global Internet **108**. (FIG. **1**, however, shows only one list provider server **120** for ease of explanation herein.) Such list provider servers would then transfer consumer records to consumer billing data protection system **100** for storage onto database **102** under the control (authorization, scheduling, validation, etc.) of list server **104**. In an alternate embodiment, list provider servers **120** would access consumer billing data protection system **100** via a dial-in line over the Public Switched Telephone Network (PSTN) **112**, rather than the global Internet **108**, to PSTN Interface **103**. In alternate embodiments, list server **104** receives and loads such consumer records from removable storage media.

Regardless of the mode used to transfer the consumer list, the consumer list comprises a plurality of consumer records, at least a portion of each being encrypted using conventional encryption techniques to safeguard the contents. The encryption process requires the use of a consumer-specific decryption key in order to access this information. In order to provide a simple decryption process, that does not require the previous exchange of a negotiated set of keys between the consumer and the marketer/telemarketer, a predetermined set of digits from the consumer's account is used as the key to decrypt the partial billing information stored in the database as well as to provide the missing billing information not yet stored in the database. In the case where the entirety of the consumer's billing information is encrypted, the consumer provided key is used to decrypt the consumer's billing information.

Encryption of the Consumer's Partial Billing Information

In one embodiment, a consumers partial billing information is encrypted prior to being transferred from a list provider to telemarketers, electronic marketers, or companies hired to perform their payment operations. This encrypted partial billing information can be decrypted only by using the "key" (e.g. the last four digits of the account number) that the consumer provides as a means of authorizing a purchase. In an alternate embodiment utilizing encryption, the list provider encrypts and transfers the consumer's complete billing information, and the "key" can be used to decrypt this complete billing information. In any event, the telemarketer, electronic marketer, or company hired to perform their payment operations is able to access the consumer's account only if it receives the consumer provided "key." Without the consumer providing this "key" to the telemarketer or electronic marketer, it is impossible to access the encrypted information.

Encryption of the Consumer's Partial Billing Information and Matchback

Alternate embodiments to lock-and-key consumer billing data protection for telemarketing and electronic marketing also include systems utilizing a "matchback" procedure. In one embodiment, a list provider transfers to a telemarketer or electronic marketer only information used to identify a consumer and to identify the credit card previously used by the consumer (e.g. type of credit card, expiration date, the first four digits of the account number, etc.), but does not transfer information sufficient to access the consumer's account. If the telemarketer or electronic marketer sends to the list provider the "key" provided by the consumer (e.g. the last four digits of the account number) and this "key" matches the corresponding part of the billing information on file with the list provider, then the list provider transfers back to the telemarketer or electronic marketer the complete billing information needed to access the consumer's account. In an alternate embodiment utilizing a "matchback" procedure, if the telemarketer or electronic marketer sends to the list provider the "key" provided by the consumer (e.g. the last four digits of the account number) and if this "key" matches the corresponding part of the billing information on file with the list provider, then the list provider transfers back to the telemarketer or electronic marketer partial billing information which can be used in conjunction with the "key" to access the consumer's account. In any event, no consumer's account is accessed unless that consumer reached into their wallet and provided the "key" to that account to the telemarketer or electronic marketer. In both of these cases, the customer billing information can be encrypted with a customer-specific encryption code and the "key" provided by the customer can then be used to decrypt the customer billing information in order to provide additional security.

In yet another alternate embodiment utilizing a "matchback" procedure, the list provider transfers complete billing information to the company hired to perform their payment operations for the telemarketer or electronic marketer. This payment company does not charge any consumer's account, however, unless this payment company receives from the telemarketer or electronic marketer the consumer's "key" (that the consumer provided the telemarketer or electronic marketer as a means of authorizing a purchase) and said "key" matches the corresponding part of the billing information on file with this payment company. Again, no consumer's account is accessed unless that consumer reached into their wallet and provided the "key" to that account to the telemarketer or electronic marketer.

Lock-and-Key Decryption/Matchback Process

FIGS. **2** and **3** are a flow charts depicting, respectively, the consumer record decryption and matchback portion of the operation of the consumer billing data protection system **100**. This process is collectively termed the billing data decryption process, which illustrates the order-entry functionality, consumer security and other advantages of consumer billing data protection system **100**.

In the various alternative embodiments noted above, the location of the consumer's partial/complete billing information and the processing of the received consumer order can be effected in any of a number of manners and in any of a number of locations. In order to illustrate the operation of the decryption process using the lock and key paradigm, the decryption process is described in the flow chart of FIG. **2** in the context of the marketer/telemarketer having the consumer record stored in database **102**, which consumer record includes partial billing information, which is encrypted using a consumer-specific cipher key. The encrypted partial billing information can be decrypted only by the use of the key provided by the consumer, and the key also constitutes the missing portion of the consumer's partial billing information.

In this embodiment of lock-and-key consumer billing data protection, the key is m alphanumeric characters of the m+p alphanumeric character billing information where consumer billing data protection system **100** has previously stored the p alphanumeric characters in encrypted form in list server **104**. In an alternate embodiment, the key is the missing m alphanumeric characters of the m+p alphanumeric character credit card billing information in addition to other data unique to the consumer or the consumer's account (such as the ACS code commonly located on credit cards), and this additional information need not be part of the billing information needed to access consumers' account.

Upon receipt of data at step **202** from the consumer which represents the key, the m alphanumeric characters of the m+p alphanumeric character billing information, the list server

104 transmits this data, along with the identity of the customer record associated with this consumer, to the decryption circuit 103 which uses the key to decrypt the encrypted customer partial billing information contained in the customer record at step 204. At step 206, the decryption circuit 103 returns the decrypted partial billing information to the list server 104 and the list server at step 208 determines whether the decrypted information constitutes the entire consumer billing information. If not, at step 210 the key is added to the partial billing information to complete the customer billing information. Once the key has been provided, the consumer billing data protection system 100 at step 212 executes the normal "back-end" processing to handle, ship—if applicable—and then bill the consumer for the purchased good(s) and/or service(s).

In order to illustrate the operation of another embodiment of the decryption process using the lock and key paradigm, the decryption process is described in the flow chart of FIG. 3 in the context of the list provider having the consumer record stored in list provider server 120, which consumer record includes partial or complete billing information, which is optionally encrypted using a consumer-specific cipher key. The list provider server 120 in this case performs the tasks noted above with respect to the consumer billing data protection system 100, as modified to accommodate the matchback process and constitutes a significant element of the consumer billing data protection system 100. The consumer billing information, if encrypted, can be decrypted only by the use of the key provided by the consumer, and the key, in the case of partial billing information, also constitutes the missing portion of the consumer's partial billing information. In the pure matchback process, the key is the consumer-specific billing information data that is provided by the consumer and without which the sales process cannot be completed.

In this embodiment of lock-and-key consumer billing data protection, the key is m alphanumeric characters of the m+p alphanumeric character billing information. In an alternate embodiment, the key is the missing m alphanumeric characters of the m+p alphanumeric character credit card billing information in addition to other data unique to the consumer or the consumer's account (such as the ACS code commonly located on credit cards), and this additional information need not be part of the billing information needed to access consumers' account. The telemarketer/marketer only has information used to identify a consumer and to identify the credit card previously used by the consumer.

Upon receipt at the list server 104 of data at step 302 from the consumer which represents the key, the m alphanumeric characters of the m+p alphanumeric character billing information, the list server 104 transmits this data, along with the identity of the customer record associated with this consumer, to the list provider server 120 which uses the key to match with the customer billing data stored in the list provider server 120 and optionally decrypt the encrypted customer partial billing information contained in the customer record at step 304. At step 306, the list provider server 120 returns the consumer's retrieved billing information and at step 308 determines whether the information constitutes the entire consumer billing information. If not, at step 310 the key is added to the partial billing information to complete the customer billing information. Once the key has been provided, the list provider server 120 at step 312 executes the normal "back-end" processing to handle, ship—if applicable—and then bill the consumer for the purchased good(s) and/or service(s).

Conclusion

While various embodiments of the present lock-and-key consumer billing data protection system having data encryption capability have been described above, it should be understood that they have been presented by way of example, and not limitation. It will be apparent to persons skilled in the relevant art(s) that various changes in form and detail can be made therein without departing from the spirit and scope of the invention. Thus, the present lock-and-key consumer billing data protection system having data encryption capability should not be limited by any of the above-described exemplary embodiments, but should be defined only in accordance with the following claims and their equivalents.

What is claimed is:

1. A method for providing a consumer billing data protection capability, *the method* comprising [the steps of]:

storing in a computer system a plurality of consumer records, each of which includes consumer identification information and encrypted partial billing information [comprising]; *wherein the encrypted partial billing information comprises an encrypted version of* a predetermined set of p alphanumeric characters of [the] *a* billing information of said consumer; *wherein the billing information is data required by a financial institution separate from the computer system to access funds from a consumer's account at the financial institution; and wherein a remaining m alphanumeric characters of the billing information are not stored in the computer system; and*

processing at said computer system an order received from a consumer, comprising:

receiving an input indicative that a consumer, corresponding to said consumer identification information stored in one of said plurality of consumer records, desires to purchase a product or service, said input including a key received from said consumer, *the key* comprising the remaining m alphanumeric characters of the billing information of said consumer, and wherein m+p is [epual] *equal* to the total number of alphanumeric characters in the billing information of said consumer;

decrypting, using said key received from said consumer, said encrypted partial billing information stored in said one of said plurality of consumer records; and

processing an order for said product or service and billing for said order using the decrypted partial billing information stored in said one of the plurality of consumer records, and said key.

2. The method of claim 1 wherein said key includes the Authenticated Content Signing (ACS) code of a credit card.

3. A method for providing a consumer billing data protection capability in a system, *the method* comprising [the steps of]:

storing in a computer system a plurality of consumer records, each of which includes consumer identification information and encrypted partial billing information [comprising]; *wherein the encrypted partial billing information comprises an encrypted version of* a predetermined set of p alphanumeric characters of [the] *a* billing information of said consumer; *wherein the billing information comprises data required by a third party to access funds from a consumer's account held by the third party; and wherein a remaining m alphanumeric characters of the billing information are not stored in the computer system; and*

processing at said computer system an order received from a consumer, comprising:

receiving an input indicative that a consumer, corresponding to said consumer identification information stored in said one of said plurality of consumer records, desires to purchase a product or service, said input including a key received from said consumer, *said key* comprising the remaining m alphanumeric characters of the billing information of said consumer, and wherein m+p is equal to the total number of alphanumeric characters in the billing information of said consumer;

decrypting, using said [key] *m alphanumeric characters* received from said consumer, said encrypted partial billing information stored in said one of said plurality of consumer records; and

processing an order for said product or service and billing for said order using said [partial] *decrypted predetermined set of p alphanumeric characters of the* billing information stored in said one of said plurality of consumer records, and said *remaining m alphanumeric characters of the billing information from said* key.

4. The method of claim **3** further comprising:

receiving data, comprising said plurality of consumer records, transmitted by a list provider.

5. The method of claim **4** wherein said key includes the Authenticated Content Signing (ACS) code of a credit card.

6. A system for providing a consumer billing data protection capability in a system that stores a plurality of consumer records, each of which includes consumer identification information and encrypted partial billing information [comprising]; *wherein the encrypted partial billing information comprises an encrypted version of* a predetermined set of p alphanumeric characters of [the] *a* billing information of said consumer, *wherein the billing information is data required by a financial institution separate from the system to access funds from a consumer's account at the financial institution; and wherein a remaining m alphanumeric characters of the billing information are not stored by the system; the system* comprising:

means for receiving an input indicative that a consumer, corresponding to said consumer identification information stored in one of said plurality of consumer records, desires to purchase a product or service, said input including a key received from said consumer, *the key* comprising the remaining m alphanumeric characters of the billing information of said consumer, and wherein m+p is equal to the total number of alphanumeric characters in the billing information of said consumer;

[means] *a decryption circuit* for decrypting, using said key received from said consumer, said encrypted partial billing information stored in said one of said plurality of consumer records; and

means for processing an order for said product or service and billing for said order using the decrypted partial billing information stored in said one of the plurality of consumer records, and said key.

7. The system of claim **6** wherein said key includes the Authenticated Content Signing (ACS) code of a credit card.

8. A system for providing a consumer billing data protection capability in a system, comprising:

database means for storing a plurality of consumer records, each of which includes consumer identification information and encrypted partial billing information [comprising]; *wherein the partial billing information comprises* a predetermined set of p alphanumeric characters of [the] *a* billing information of said consumer; *wherein the billing information is data required by a financial institution separate from the system to access funds from a consumer's account at the financial institution; and wherein a remaining m alphanumeric characters of the billing information are not stored in the computer system;*

list server means for receiving an input indicative that a consumer, corresponding to said consumer identification information stored in said one of said plurality of consumer records, desires to purchase a product or service, said input including a key received from said consumer, *the key* comprising the remaining m alphanumeric characters of the billing information of said consumer, and wherein m+p is equal to the total number of alphanumeric characters in the billing information of said consumer;

decryption *circuit* means *for* decrypting, using said key received from said consumer, said encrypted partial billing information stored in said one of said plurality of consumer records; and

list provider server means for processing an order for said product or service and billing for said order using said partial billing information stored in said one of said plurality of consumer records, and said key.

9. The system of claim **8** further comprising:

means for receiving data, comprising said plurality of consumer records, transmitted by a list provider.

10. The [method] *system* of claim **9** wherein said key includes the Authenticated Content Signing (ACS) code of a credit card.

11. A method for providing a consumer billing data protection capability, comprising [the steps of]:

storing in a computer system a plurality of consumer records, each of which includes consumer identification information and encrypted partial billing information [comprising a]; *wherein the encrypted partial billing information comprises an encrypted* predetermined set of p alphanumeric characters of [the] *a* billing information of said consumer; *wherein the billing information is data required by a financial institution separate from the computer system to access funds from a consumer's account at the financial institution; and wherein a remaining m alphanumeric characters of the billing information are not stored in the computer system; and*

processing at said computer system an order received from a consumer, comprising:

receiving an input indicative that a consumer, corresponding to said consumer identification information stored in one of said plurality of consumer records, desires to purchase a product or service, said input including a key received from said consumer, *the key* comprising the remaining m alphanumeric characters of the billing information of said consumer, and wherein m+p is equal to the total number of alphanumeric characters in the billing information of said consumer;

accessing, using said key received from said consumer, said consumer billing information stored in said one of said plurality of consumer records; and

processing an order for said product or service and billing for said order using the consumer billing information stored in said one of the plurality of consumer records, and said key.

12. The method of claim **11** wherein said key includes the Authenticated Content Signing (ACS) code of a credit card.

13. The method of claim 11 further comprising:

storing a plurality of consumer records, each of which includes consumer identification information and consumer billing information.

14. A system for providing a consumer billing data protection capability in a system that stores a plurality of consumer records, each of which includes consumer identification information and consumer billing information [comprising]; *wherein the consumer billing information comprises* a predetermined set of p alphanumeric characters of [the] *a complete* billing information of said consumer, *wherein the complete billing information is data required by a financial institution separate from the system to access funds from a consumer's account at the financial institution; and wherein a remaining m alphanumeric characters of the complete billing information are not stored in the computer system; the system* comprising [the steps of]:

means for receiving an input indicative that a consumer, corresponding to said consumer identification information stored in one of said plurality of consumer records, desires to purchase a product or service, said input including a key received from said consumer, *the key* comprising the remaining m alphanumeric characters of the *complete* billing information of said consumer and wherein m+p is equal to the total number of alphanumeric characters in the *complete* billing information of said consumer;

[means] *a decryption circuit* for accessing, using said key received from said consumer, said consumer billing information stored in said one of said plurality of consumer records; and

means for processing an order for said product or service and billing for said order using the consumer billing information stored in said one of the plurality of consumer records, and said key.

15. The system of claim 14 wherein said key includes the Authenticated Content Signing (ACS) code of a credit card.

16. The system of claim 14 further comprising:

means for storing a plurality of consumer records, each of which includes consumer identification information and consumer billing information.

17. A method for providing a consumer billing data protection capability, comprising:

storing in a computer system a plurality of consumer records, each of which includes consumer identification information and encrypted partial billing information; wherein the encrypted partial billing information includes an encrypted copy of a first portion of the billing information of said consumer comprising a predetermined set of p alphanumeric characters of a billing information of said consumer; wherein the billing information is data required by a financial institution separate from the computer system to charge a consumer's account; and wherein a second portion of the billing information that completes the billing information when combined with the first portion is not stored in the computer system; and

processing at said computer system an order received from a consumer, comprising:

receiving a key from said consumer, the key including the second portion of the billing information, the second portion comprising the remaining m alphanumeric characters of the billing information, wherein m+p is equal to the total number of alphanumeric characters in the billing information of said consumer;

decrypting said encrypted partial billing information stored in said one of said plurality of consumer records using said key received from said consumer; and

billing said consumer for said order using the first portion of the billing information and the second portion of the billing information.

18. The method of claim 17 wherein said key includes the Authenticated Content Signing (ACS) code of a credit card.

19. A method for providing a consumer billing data protection capability in a system, comprising:

storing in a computer system a plurality of consumer records, each of which includes consumer identification information and encrypted partial billing information; wherein the encrypted partial billing information comprises an encrypted version of a predetermined set of p alphanumeric characters of a p+m alphanumeric characters of the billing information of said consumer required by a third party to access funds from a consumer's account held by the third party; wherein m+p is equal to the total number of alphanumeric characters in the billing information of said consumer, and wherein a remaining m alphanumeric characters of the m+p alphanumeric characters of the billing information are not stored in the computer system; and

processing at said computer system an order received from a consumer, comprising:

receiving a key from said consumer, the key comprising the remaining m alphanumeric characters of the billing information of said consumer;

decrypting said p alphanumeric characters, using the m alphanumeric characters from said key; and

billing said consumer for said order using said decrypted p alphanumeric characters and said m alphanumeric characters from said key.

20. The method of claim 19 further comprising:

receiving data, comprising said plurality of consumer records, transmitted by a list provider.

21. The method of claim 19 wherein said key includes the Authenticated Content Signing (ACS) code of a credit card.

22. A system for providing a consumer billing data protection capability in a system that stores a plurality of consumer records, each of which includes consumer identification information and encrypted partial billing information wherein the encrypted partial billing information comprises an encrypted version of a predetermined set of p alphanumeric characters of a billing information of said consumers, wherein the billing information is data required by a financial institution separate from the system to access funds from a consumer's account at the financial institution, and wherein a remaining m alphanumeric characters of the billing information are not stored by the system; the system comprising:

means for receiving a key from a consumer, the key comprising the remaining m alphanumeric characters of the billing information of said consumer, and wherein m+p is equal to the total number of alphanumeric characters in the billing information of said consumer;

a decryption circuit for decrypting, using said key received from said consumer, said encrypted partial billing information stored in said one of said plurality of consumer records; and

means for billing said consumer for an order for a product or service using the decrypted partial billing information and said key.

23. The system of claim 22 wherein said key includes the Authenticated Content Signing (ACS) code of a credit card.

24. A system for providing a consumer billing data protection capability in a system, comprising:

database means for storing a plurality of consumer records, each of which includes consumer identification information and encrypted partial billing information; wherein the encrypted partial billing information comprises an encrypted version of a first portion of a billing information of said consumers, the first portion comprising a predetermined set of p alphanumeric characters of the billing information of said consumers; wherein m+p is equal to the total number of alphanumeric characters in the billing information of said consumers; wherein the billing information is data required by a financial institution separate from the system to charge a consumer's account; wherein a second portion of the billing information comprising a remaining m alphanumeric characters of the billing information of said consumers is not stored in the computer system, and wherein the first portion and the second portion combined constitute the entire billing information;

list server means for receiving a key from a consumer, the key including the second portion of the billing information of said consumer comprising the remaining m alphanumeric characters of the billing information;

decryption circuit means for decrypting, using the second portion of the billing information, said encrypted partial billing information stored in said one of said plurality of consumer records; and

list provider server means for billing said consumer for an order for a product or service using said decrypted partial billing information and said second portion of the billing information.

25. The system of claim 24 further comprising:

means for receiving data, comprising said plurality of consumer records, transmitted by a list provider.

26. The system of claim 24 wherein said key includes the Authenticated Content Signing (ACS) code of a credit card.

27. A method for providing a consumer billing data protection capability, comprising:

storing in a computer system a plurality of consumer records, each of which includes consumer identification information and encrypted partial billing information; wherein the encrypted partial billing information comprises an encrypted version of a predetermined set of p alphanumeric characters of a complete billing information of said consumers; wherein m+p is equal to the total number of alphanumeric characters in the billing information of said consumers; wherein the complete billing information is data required by a financial institution separate from the computer system to access funds from a consumer's account at the financial institution; and wherein a remaining m alphanumeric characters of the complete billing information are not stored in the computer system; and

processing at said computer system an order received from a consumer, comprising:

receiving a key from said consumer, the key comprising the remaining m alphanumeric characters of the complete billing information of said consumer, and wherein m+p is equal to the total number of alphanumeric characters in the complete billing information of said consumer;

accessing, using said key received from said consumer, said partial billing information stored in said one of said plurality of consumer records; and

billing said consumer for said order using the complete billing information by combining the p alphanumeric characters from said partial billing information stored in said one of the plurality of consumer records, and the m alphanumeric characters from said key.

28. The method of claim 27 wherein said key includes the Authenticated Content Signing (ACS) code of a credit card.

29. The method of claim 27 further comprising:

storing a plurality of consumer records, each of which includes consumer identification information and encrypted partial billing information.

30. A system for providing a consumer billing data protection capability in a system that stores a plurality of consumer records, each of which includes consumer identification information and encrypted consumer billing information; wherein the encrypted consumer billing information comprises a predetermined set of p alphanumeric characters of a complete billing information of said consumers, wherein the complete billing information is data required by a financial institution separate from the system to access funds from a consumer's account at the financial institution, and wherein a remaining m alphanumeric characters of the complete billing information are not stored in the computer system; the system comprising:

means for receiving a key from a consumer, the key comprising the remaining m alphanumeric characters of the billing information of said consumer and wherein m+p is equal to the total number of alphanumeric characters in the billing information of said consumer;

a decryption circuit for accessing, using said key received from said consumer, said consumer billing information stored in said one of said plurality of consumer records; and

means for billing said consumer for an order for a product or service using the consumer billing information stored in said one of the plurality of consumer records, and said key.

31. The system of claim 30 wherein said key includes the Authenticated Content Signing (ACS) code of a credit card.

32. The system of claim 30 further comprising:

means for storing a plurality of consumer records, each of which includes consumer identification information and consumer billing information.

33. A tangible computer-readable storage medium having computer-executable instructions stored thereon, execution of which by a computer system causes the computer system to perform operations in decrypting and completing partial billing information stored in a plurality of consumer records, each consumer record including consumer identification information and encrypted partial billing information; wherein the encrypted partial billing information comprises an encrypted version of a predetermined set of p alphanumeric characters of a billing information of said consumers; wherein the billing information is data required by a financial institution separate from the computer system to access funds from a consumer's account at the financial institution; and wherein a remaining m alphanumeric characters of the billing information are not stored in the computer system; the operations comprising:

receiving a key from a consumer, the key comprising the remaining m alphanumeric characters of the billing information of said consumer, and wherein m+p is equal to the total number of alphanumeric characters in the billing information of said consumer;

decrypting, using said key received from said consumer, said encrypted partial billing information stored in said one of said plurality of consumer records; and

completing the billing information by combining the key with the decrypted partial billing information.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : RE43,845 E
APPLICATION NO. : 12/118663
DATED : December 4, 2012
INVENTOR(S) : Rothfarb

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

The Title page, showing the illustrative figures, should be deleted and substitute therefor the attached Title page.

In the Drawings:

Delete figs. 1 - 3 and substitute therefor the drawing sheets, consisting of figs. 1 - 3 as shown on the attached pages.

In the Specifications:

In Column 6, Line 42, delete "(PBX) 109" and insert -- (PBX) 105 --, therefor.

In Column 6, Lines 63-64, delete "Public Switched Telephone Network 105," and insert -- Public Switched Telephone Network 112, --, therefor.

In Column 7, Line 14, delete "PSTN Interface 103." and insert -- PSTN Interface 113. --, therefor.

Signed and Sealed this
Twentieth Day of August, 2013

Teresa Stanek Rea
Acting Director of the United States Patent and Trademark Office

(19) **United States**
(12) **Reissued Patent**
Rothfarb

(10) **Patent Number: US RE43,845 E**
(45) **Date of Reissued Patent: Dec. 4, 2012**

(54) **LOCK-AND-KEY CONSUMER BILLING DATA PROTECTION SYSTEM HAVING DATA ENCRYPTION CAPABILITY**

(75) Inventor: **Neil Barry Rothfarb**, West Hartford, CT (US)

(73) Assignee: **Nebarb Software Foundation L.L.C.**, Wilmington, DE (US)

(21) Appl. No.: **12/118,663**

(22) Filed: **May 9, 2008**

Related U.S. Patent Documents

Reissue of:

(64) Patent No.: **7,043,452**
Issued: **May 9, 2006**
Appl. No.: **10/160,765**
Filed: **May 31, 2002**

U.S. Applications:

(63) Continuation-in-part of application No. 10/146,252, filed on May 15, 2002, and a continuation-in-part of application No. 10/146,249, filed on May 15, 2002.

(51) **Int. Cl.**
G06F 21/00 (2006.01)

(52) **U.S. Cl.** **705/50**; 705/2; 705/51; 705/77; 705/40; 380/203; 713/165; 713/200

(58) **Field of Classification Search** 705/40, 705/50
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,123,747	A		10/1978	Lancto
5,432,851	A		7/1995	Scheidt
5,455,953	A		10/1995	Russell
5,590,197	A		12/1996	Chen
5,706,442	A		1/1998	Anderson
5,727,163	A		3/1998	Bezos
5,745,556	A	*	4/1998	Ronen 379/127.05
5,748,718	A		5/1998	Manicone
5,960,411	A	*	9/1999	Hartman et al. 705/26
6,128,603	A		10/2000	Dent
6,408,284	B1		6/2002	Hilt
6,676,016	B1		1/2004	Coskrey, IV
6,839,687	B1		1/2005	Dent

(Continued)

FOREIGN PATENT DOCUMENTS

JP	363316626	A	12/1988

OTHER PUBLICATIONS

"The Bank Credit Card Business," 2d ed., American Bankers Association, Washington, D.C., 1996, 243 pages.

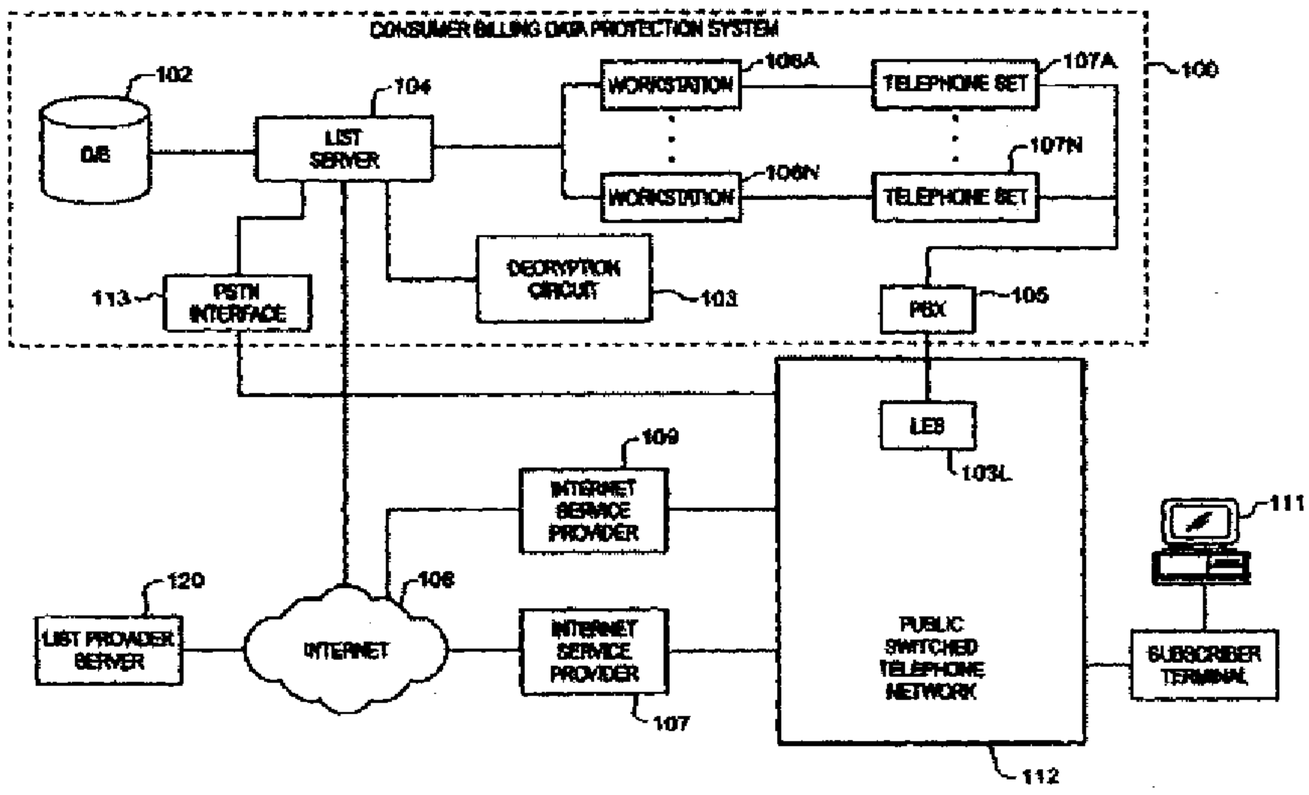
(Continued)

Primary Examiner — Jacob C. Coppola

(57) **ABSTRACT**

A "lock-and-key" consumer billing data protection capability is provided to telemarketing and electronic marketing systems which are based upon previously-acquired consumer lists. The lists contain encrypted partial billing information for each consumer, which is insufficient to access the consumer's account. Thus, at the time a consumer is offered a product or service, the telemarketer, the electronic marketer, and any entity hired to perform billing operations for such consumer purchases all remain "locked" out from accessing the consumer's account. When the consumer wishes to authorize the purchase of an offered product or service, the consumer must provide the "key" to the consumer's account, which is the key necessary to decrypt the encrypted partial billing information and also the missing billing information not acquired from the list provider.

33 Claims, 3 Drawing Sheets



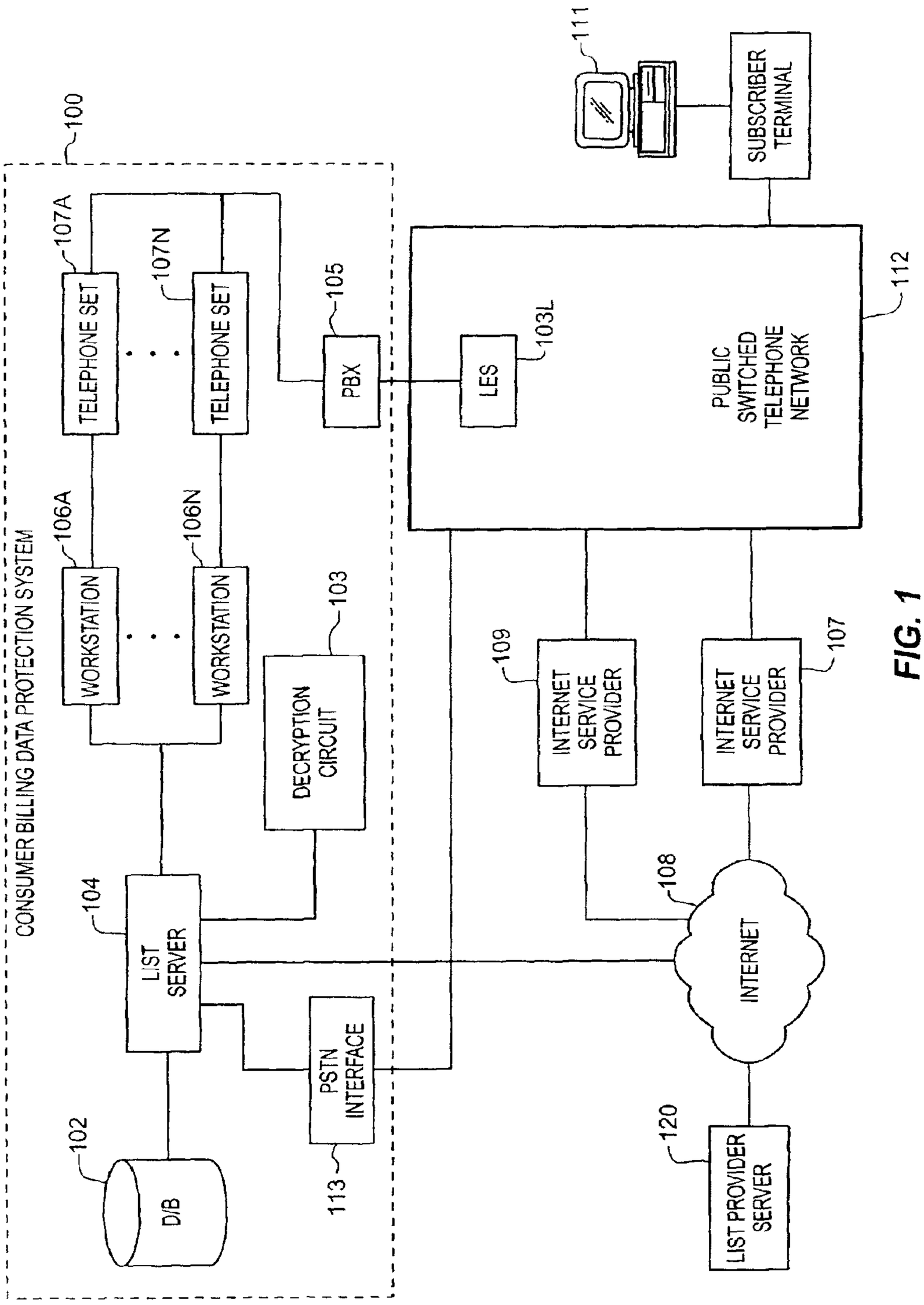

100
CONSUMER BILLING DATA PROTECTION SYSTEM
107A
TELEPHONE SET
107N
TELEPHONE SET
105
PBX
103L
LES
111
SUBSCRIBER TERMINAL
112
PUBLIC SWITCHED TELEPHONE NETWORK
106A
WORKSTATION
106N
WORKSTATION
103
DECRYPTION CIRCUIT
109
INTERNET SERVICE PROVIDER
107
INTERNET SERVICE PROVIDER
104
LIST SERVER
108
INTERNET
102
D/B
PSTN INTERFACE
113
120
LIST PROVIDER SERVER

FIG. 1

FIG. 2

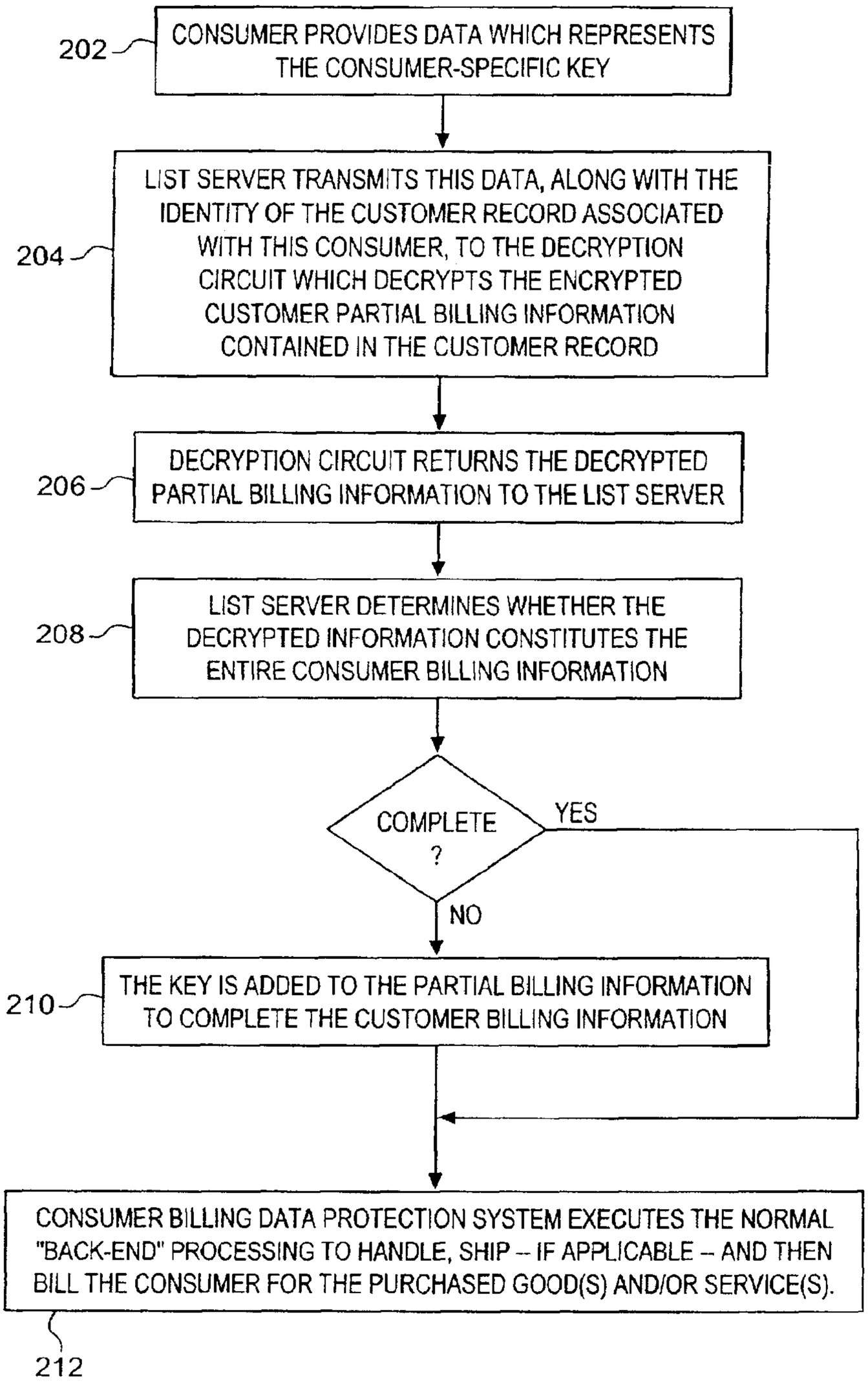
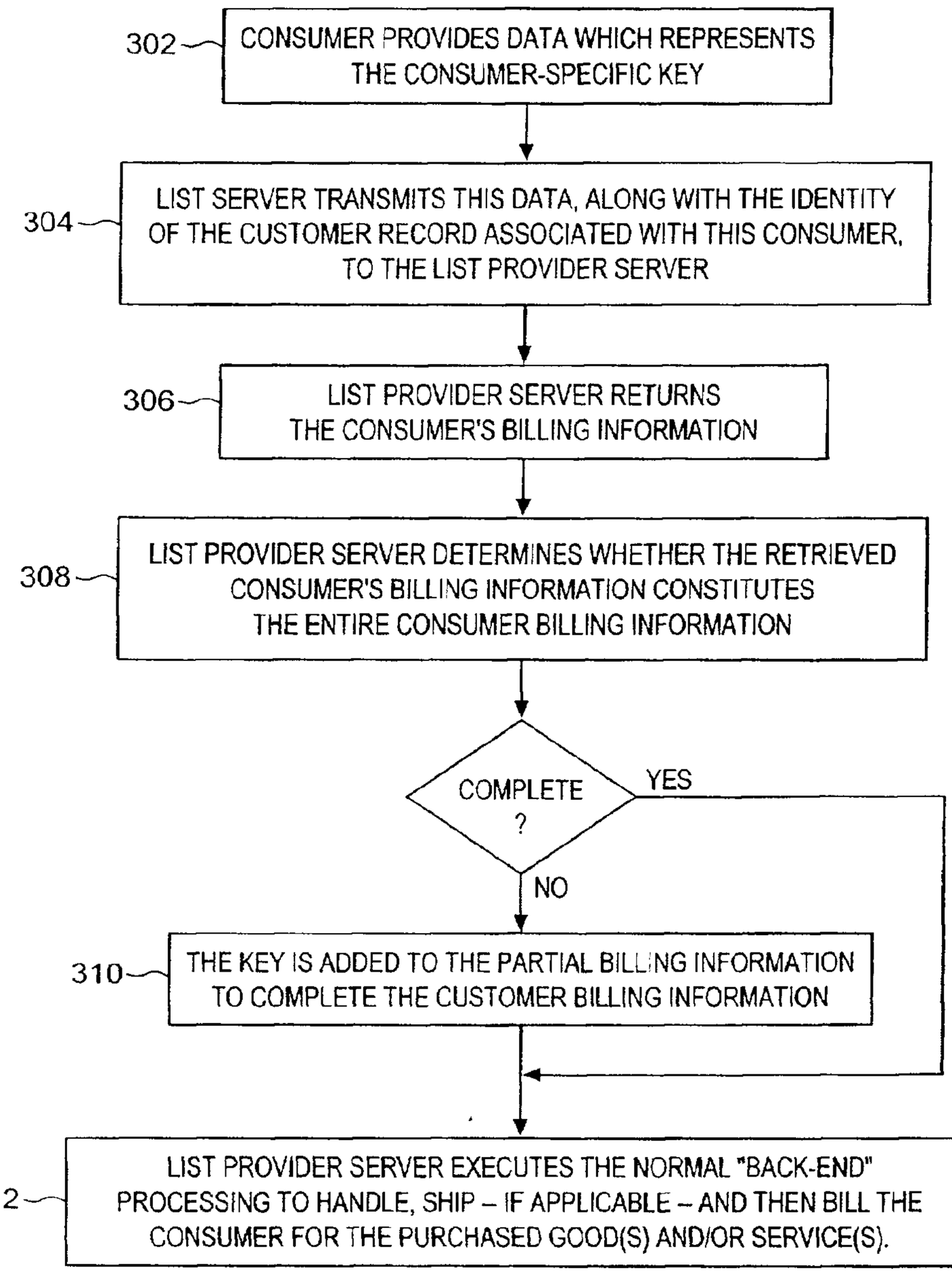

202
CONSUMER PROVIDES DATA WHICH REPRESENTS THE CONSUMER-SPECIFIC KEY
204
LIST SERVER TRANSMITS THIS DATA, ALONG WITH THE IDENTITY OF THE CUSTOMER RECORD ASSOCIATED WITH THIS CONSUMER, TO THE DECRYPTION CIRCUIT WHICH DECRYPTS THE ENCRYPTED CUSTOMER PARTIAL BILLING INFORMATION CONTAINED IN THE CUSTOMER RECORD
206
DECRYPTION CIRCUIT RETURNS THE DECRYPTED PARTIAL BILLING INFORMATION TO THE LIST SERVER
208
LIST SERVER DETERMINES WHETHER THE DECRYPTED INFORMATION CONSTITUTES THE ENTIRE CONSUMER BILLING INFORMATION
COMPLETE ?
YES
NO
210
THE KEY IS ADDED TO THE PARTIAL BILLING INFORMATION TO COMPLETE THE CUSTOMER BILLING INFORMATION
CONSUMER BILLING DATA PROTECTION SYSTEM EXECUTES THE NORMAL "BACK-END" PROCESSING TO HANDLE, SHIP -- IF APPLICABLE -- AND THEN BILL THE CONSUMER FOR THE PURCHASED GOOD(S) AND/OR SERVICE(S).
212

FIG. 3


302
CONSUMER PROVIDES DATA WHICH REPRESENTS THE CONSUMER-SPECIFIC KEY
304
LIST SERVER TRANSMITS THIS DATA, ALONG WITH THE IDENTITY OF THE CUSTOMER RECORD ASSOCIATED WITH THIS CONSUMER, TO THE LIST PROVIDER SERVER
306
LIST PROVIDER SERVER RETURNS THE CONSUMER'S BILLING INFORMATION
308
LIST PROVIDER SERVER DETERMINES WHETHER THE RETRIEVED CONSUMER'S BILLING INFORMATION CONSTITUTES THE ENTIRE CONSUMER BILLING INFORMATION
COMPLETE ?
YES
NO
310
THE KEY IS ADDED TO THE PARTIAL BILLING INFORMATION TO COMPLETE THE CUSTOMER BILLING INFORMATION
312
LIST PROVIDER SERVER EXECUTES THE NORMAL "BACK-END" PROCESSING TO HANDLE, SHIP – IF APPLICABLE – AND THEN BILL THE CONSUMER FOR THE PURCHASED GOOD(S) AND/OR SERVICE(S).