US005671279A

United States Patent [19]
Elgamal

[11] **Patent Number: 5,671,279**
[45] **Date of Patent: Sep. 23, 1997**

[54] **ELECTRONIC COMMERCE USING A SECURE COURIER SYSTEM**

[75] Inventor: **Taher Elgamal**, Palo Alto, Calif.

[73] Assignee: **Netscape Communications Corporation**, Mountain View, Calif.

[21] Appl. No.: **555,976**

[22] Filed: **Nov. 13, 1995**

[51] **Int. Cl.**^{6} **H04K 1/00**

[52] **U.S. Cl.** **380/23**; 380/25; 380/4; 380/49; 380/29; 380/30

[58] **Field of Search** 380/23, 24, 25, 380/4, 3, 49, 29, 30

[56] **References Cited**

PUBLICATIONS

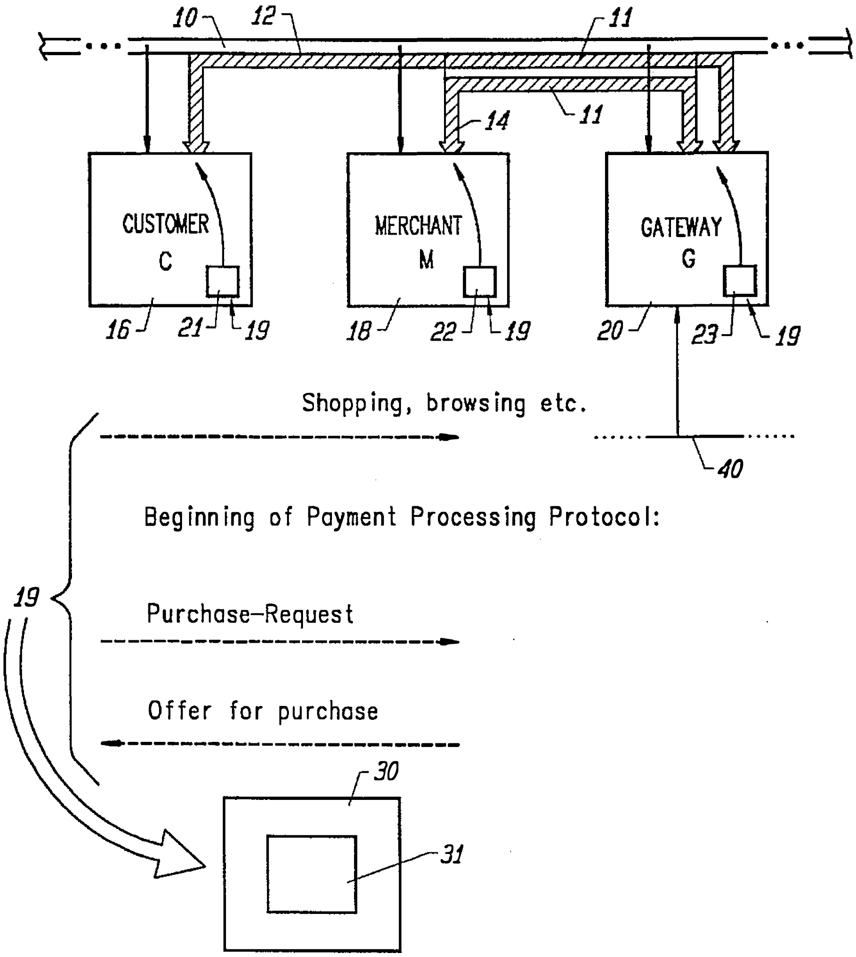
Linehan & Taudik, IBM Research, Jul., 1995, "Internet Keyed Payments Protocol".
Wired, Oct. 1995, "Scans, Banking with First Virtual".
MacWorld, Nov. 1995, "Money on the Line", p. 114.
Borenstein & Rose, First Virtual Holdings, Oct., 1994, "The application/green–commerce MIME Content–type".
Stein et al., "The Green Commercial Model", Oct., 1994.
"Encryption and Internet Commerce," First Virtual Holdings, Inc., 1995.
Secure Transaction Technology, Version 1.0, "Securing the 'Net".
"Secure Electronic Payment Protocol," Draft Version 1.1, Sep. 29, 1995, MasterCard.

Primary Examiner—David C. Cain
Attorney, Agent, or Firm—Michael A. Glenn

[57] **ABSTRACT**

A courier electronic payment system provides customers, merchants, and banks with a secure mechanism for using a public network as a platform for credit card payment services. The system governs the relationship between a Customer, Merchant, and Acquirer Gateway to perform credit card purchases over such networks as the Internet. The system uses a secure connection to simplify the problem of Internet-based financial transactions in accordance with an electronic payment protocol that secures credit card payments and certifies infrastructure that is required to enable all of the parties to participate in the electronic commerce, as well as to provide the necessary formats and interfaces between the different modules and systems.

36 Claims, 3 Drawing Sheets



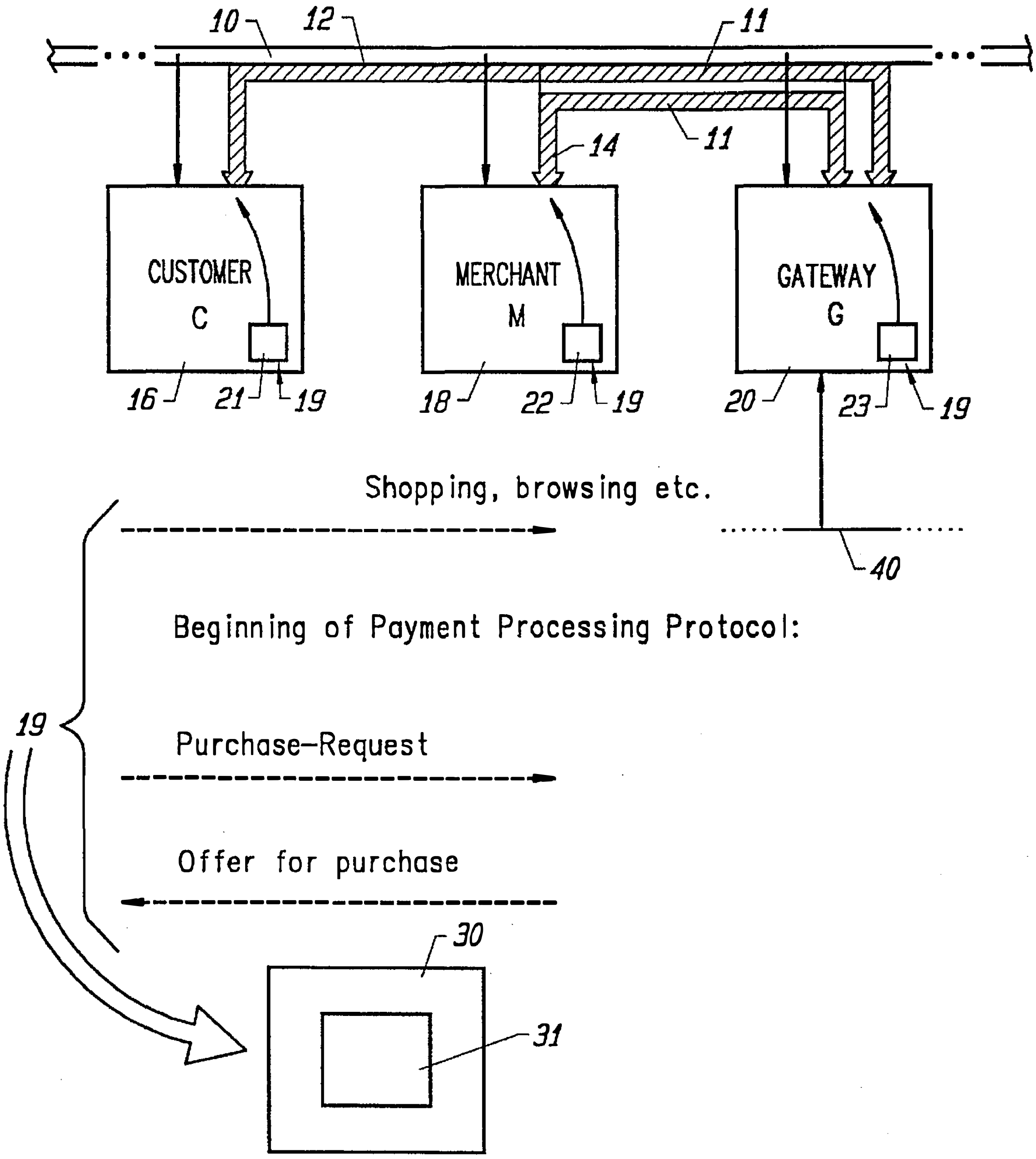

10
12
11
14
11
CUSTOMER
C
MERCHANT
M
GATEWAY
G
16
21
19
18
22
19
20
23
19
Shopping, browsing etc.
40
Beginning of Payment Processing Protocol:
19
Purchase-Request
Offer for purchase
30
31

FIG. 1

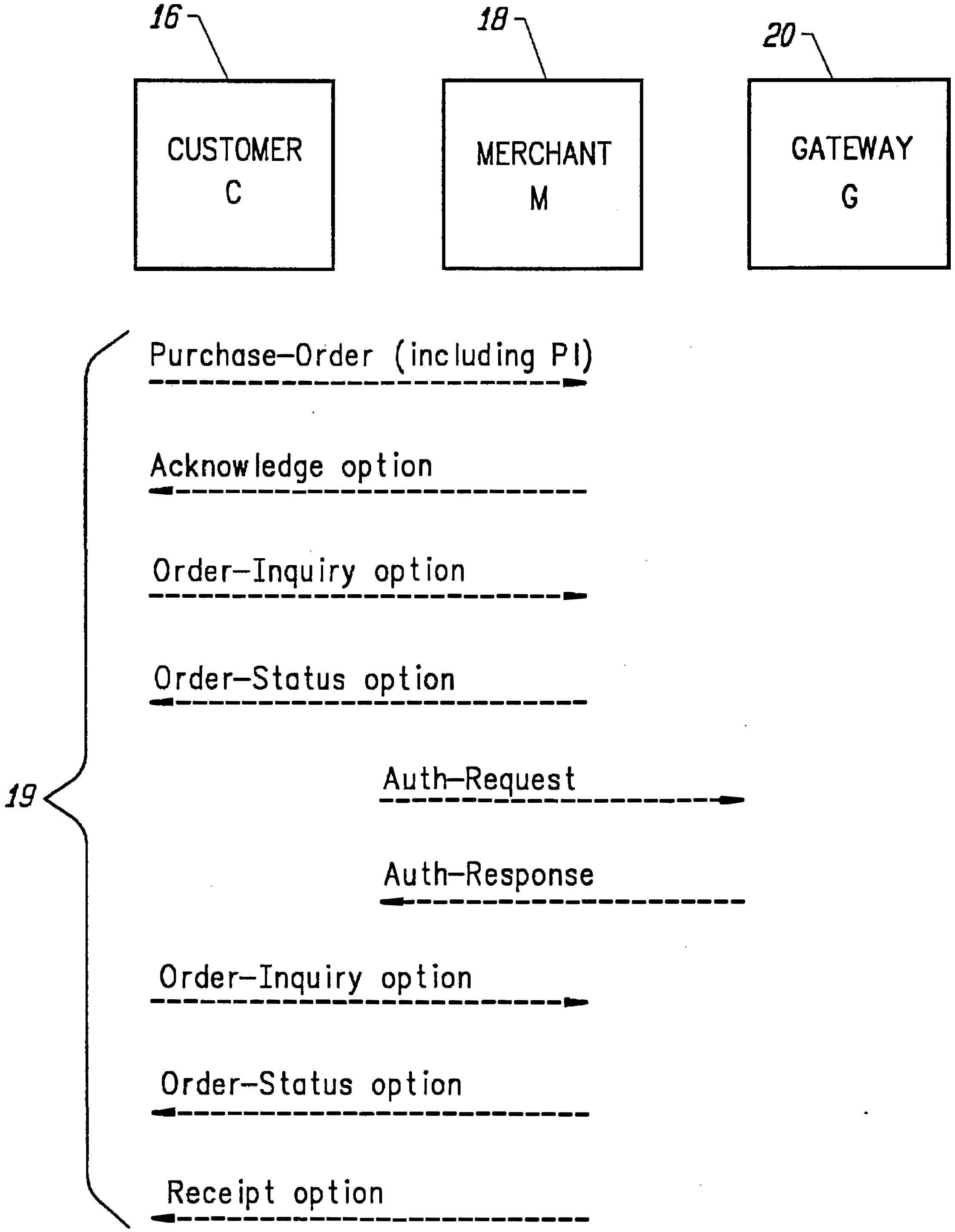

16
CUSTOMER
C
18
MERCHANT
M
20
GATEWAY
G
19
Purchase–Order (including PI)
Acknowledge option
Order–Inquiry option
Order–Status option
Auth–Request
Auth–Response
Order–Inquiry option
Order–Status option
Receipt option

FIG. 2

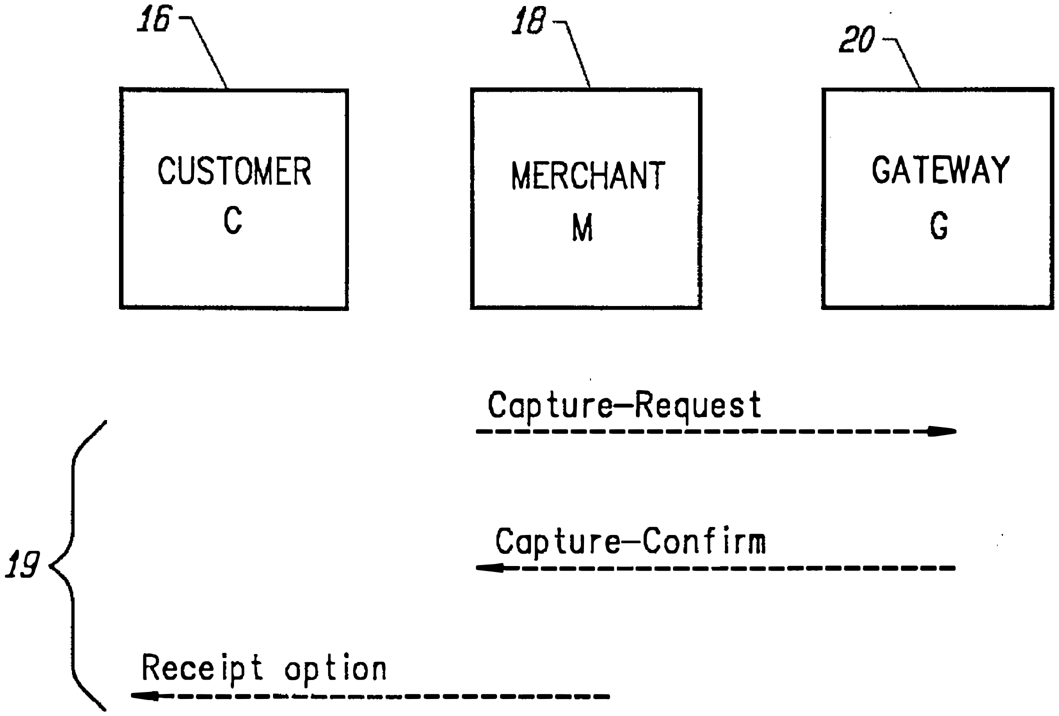

16
18
20
CUSTOMER
C
MERCHANT
M
GATEWAY
G
Capture–Request
Capture–Confirm
19
Receipt option

FIG. 3

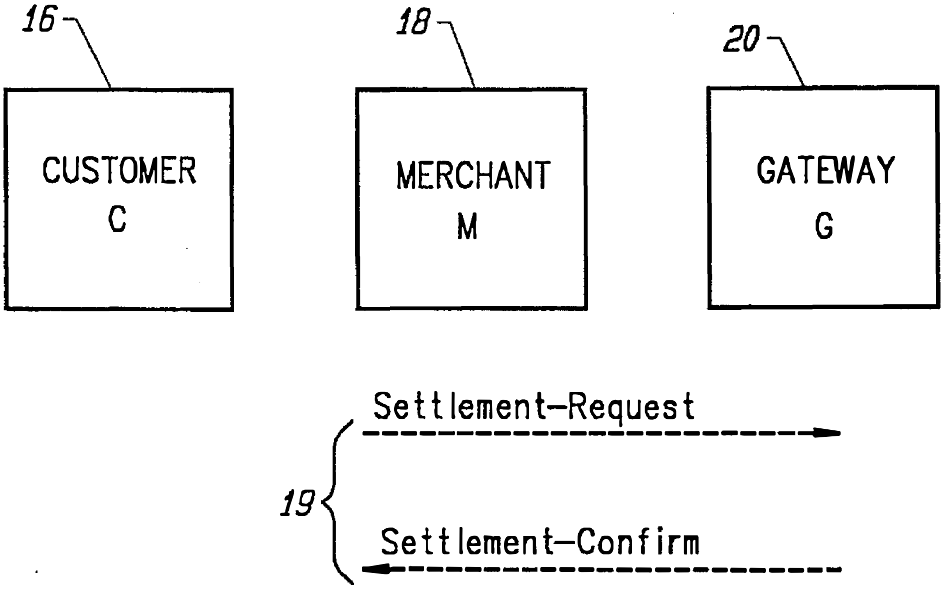

16
18
20
CUSTOMER
C
MERCHANT
M
GATEWAY
G
Settlement–Request
19
Settlement–Confirm

FIG. 4

ELECTRONIC COMMERCE USING A SECURE COURIER SYSTEM

BACKGROUND OF THE INVENTION

1. Technical Field

The invention relates to the processing of commercial transactions. More particularly, the invention relates to the secure processing of on-line commercial transactions.

2. Description of the Prior Art

A fast-growing trend on the Internet is the ordering and provision of information, goods, and services via the World Wide Web, electronic mail, and other means. A key issue for related to such electronic commerce is the authorization and satisfaction of payment for such goods and services in an efficient, reliable, and secure manner. A number of organizations have addressed this issue by establishing proprietary payment systems which vary widely in design, performance, and security features.

See, for example M. Linehan, G. Tsudik, *Internet Keyed Payments Protocol* (*iKP*), Internet-Draft <draft-tsudik-ikp-00.txt> (July 1995) (an architecture for secure payments that involves three or more participants in which a base protocol includes a number of options that can be selected to meet varying business or security requirements, for example by applying cryptographic techniques to minimize potential risks concerning payments over the open Internet).

See, also L. Stein, E. Stefferud, N. Borenstein, M. Rose, *The Green Commerce Model,* First Virtual Holdings, Inc., October 1994 (http://www.infohaus.com); N. Borenstein, M. Rose, *The application/green-commerce MIME Content-type,* First Virtual Holdings, Inc., October 1994 (http://www.infohaus.com); and *Encryption and Internet Commerce,* First Virtual Holdings, Inc., 1995 (http://www.infohaus.com); and First Virtual Holdings, Inc., Wired, pp. 51 (October 1995), MacWorld, pp. 114 (November 1995) (an on-line transaction clearing house in which accounts are established off-line via telephone, and in which a transaction requires an account number, where each transaction is confirmed by the clearing house via email); CyberCash, MacWorld, pp. 114 (November 1995) (an electronic payment system that uses cryptography to prevent eavesdroppers from stealing and unscrupulous merchants from overcharging); NetCheque, University of Southern California, MacWorld, pp. 114 (November 1995) (an on-line checking system in which an account holder can send an electronic document that a recipient can deposit electronically into a bank account as a check, where the document contains the name of the payer, financial institution, payer's account number, payee's name, and amount of check, and which includes a digital signature of the payer and which may include a digital signature of a payee); and DigiCash, MacWorld, pp. 114 (November 1995) (an Internet payment systems, referred to as eCash, that provides digital money without an audit trail, thereby protecting the privacy of parties to the transaction).

Additionally, electronic commerce systems have been proposed by Visa International Service Association in collaboration with Microsoft Corporation (Secure Transaction Technology, using digital signature to authenticate a credit card and merchant decal; see http://www.visa.com); and MasterCard (Secure Electronic Payment Protocol, a collection of elements including an authorized holder of a bankcard supported by an issuer and registered to perform electronic commerce, a merchant of goods, services, and/or information who accepts payment from the holder electronically, a MasterCard member financial institution that supports merchants by providing service for processing credit card based transactions, a certificate management system that provides for the creation and distribution of electronic certificates for merchants, financial institutions, and cardholders, and a network to interface the merchants, financial institutions, cardholders, and certificate management system; see http://www.mastercard.com). Payments in the real world are accomplished via such mechanisms as cash, checks, credit and debit cards, money, and postal orders. Electronic equivalents of all these payment systems are being developed. For example, iKP, ibid., addresses a subset of these mechanisms that involve direct payment transfers among accounts maintained by banks and other financial organizations. This includes credit and debit card transactions, as well as electronic check clearing, but excludes electronic cash and money orders because these require very different mechanisms. The stated goal of iKP is to enable Internet-based secure electronic payments while using the existing financial infrastructure for payment authorization and clearance. The intent is to avoid completely, or at least minimize, changes to the existing financial infrastructure outside of the Internet.

Payment systems incorporate tradeoffs among cost, timeliness, efficiency, reliability, risk management, and convenience. For example, some systems attempt to suppress fraud by inducing payment delays. Security in payment systems means minimizing risk to a level acceptable to participants. Risk management in existing systems is accomplished by varying combinations of technology, payment practices, insurance, education, laws, contracts, and enforcement. The state of the art uses cryptographic technology, such as public-key cryptography, to support payments among parties who have no preexisting relationship in a scalable manner.

Many existing cryptographic protocols, such as SSL (K. E. B. Hickman, *The SSL Protocol,* Internet Draft <draft-hickman-netscape-ssl-00.txt>, April 1995), SHTTP (E. Rescorla, A. Schiffman, *The Secure HyperText Transfer Protocol,* Internet Draft <draft-rescorla-shttp-0.txt>, December 1994), PEM (J. Linn, *Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures,* RFC 1421, February 1993), MOSS (S. Crocker, N. Freed, J. Galvin, *MIME Object Security Services,* Internet Draft <draft-ietf-pem-mime-08.txt>, March 1995), and IPSP (R. Atkinson, *Security Architecture for the Internet Protocol,* Internet Draft <draft-ietf-ipsec-arch-02.txt>, May 1995), provide security functions for pairwise communication. For example, SSL provides privacy and authentication, but no non-repudiation, between clients and servers of application-layer protocols such as HTTP and FTP. Many payment systems involve three or more parties, i.e. buyer, seller, and bank. In such systems, certain types of risk can be ameliorated by sharing sensitive information only among a subset of the parties. For example, credit card fraud can be reduced by transmitting credit card account numbers between buyers and banks without revealing them to sellers.

As the Internet continues to grow, a significant portion of the economy may become inextricably interwoven with Internet-based on-line transactions. It would therefore be advantageous to provide a secure, reliable, and efficient mechanism for implementing transactions associated with on-line commerce.

SUMMARY OF THE INVENTION

A courier electronic payment system provides customers, merchants, and banks with a secure mechanism for using a

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | sales@docketalarm.com | 1-866-77-FASTCASE

Smarter legal research.