

Identity theft erodes consumer trust

53%¹ of consumer fraud was internet-related

Insufficient identity validation

Internet fraud costs² more than US\$2.6 billion in 2004.

PayTC™ key security features:



Hardware security

Registration and activation

Deactivation

Inaccessible personal data

End-to-end encryption of data

Password access

Intrusion detection

Non-repudiation

Identity theft is the single biggest single threat to consumer e-commerce, occurring when key personal information is acquired by hostile third parties. The problem is exacerbated by the fact that credit or debit card information is provided to all members of the online payment chain (merchants, gateways, processors and banks), creating several independent weaknesses in the online security of confidential consumer information. Some consumers have never trusted online transactions but highly publicized cases of identity theft erode what little consumer confidence there was in the security of online data.

Once personal data is compromised there is no reliable way to validate the identity of the consumer. Although most online merchants insist on corroborating evidence in addition to a credit card number, this approach is insufficient. Fraud costs merchants and banks hundreds of millions of dollars each year, is an inconvenience to existing online consumers and is a deterrent to those who would be.

The Payment Token Card (PayTC™), which forms part of the TCC Online Payment System (TCCOPS³), is a USB device small enough to fit on a keychain. As the online analogue of the credit card itself, the PayTC™ encapsulates credit card information in a secure, tamper-proof physical device with the following key security features:

- As a hardware device the PayTC™ can only be provided to the consumer by the issuing credit or debit card authority.
- The PayTC™ is unusable without proper registration and activation by the user, precluding fraud before the device is delivered.
- The PayTC™ can be deactivated by the user or revoked by the card issuer should fraudulent activity be suspected.
- Data held inside the PayTC™ is not directly accessible because all personal data is encrypted on the device. Only a trusted authority, such as the bank, can decrypt the credit or debit card information. Not even the consumer can decrypt the information.
- The PayTC™ never provides a credit or debit card number or the consumer's personal information in the "clear"; it only provides data as encrypted data packages. Not even the merchant or the payment gateway can read the credit card information.
- Access to the PayTC™ device is secured with a password known only to the consumer who owns it. However, even the consumer can not read the credit or debit card information.
- If the PayTC™ is tampered with or if multiple password attempts fail, TCCOPS will disable the device and/or revoke its registration.
- As a physical device accessible only with a password, the PayTC™ ensures non-repudiation of the transaction by the consumer.

¹ National and State Trends in Identity Theft, Federal Trade Commission, 2004.

² [Online fraud costs \\$2.6 billion in 2004 - MSNBC News.](#)

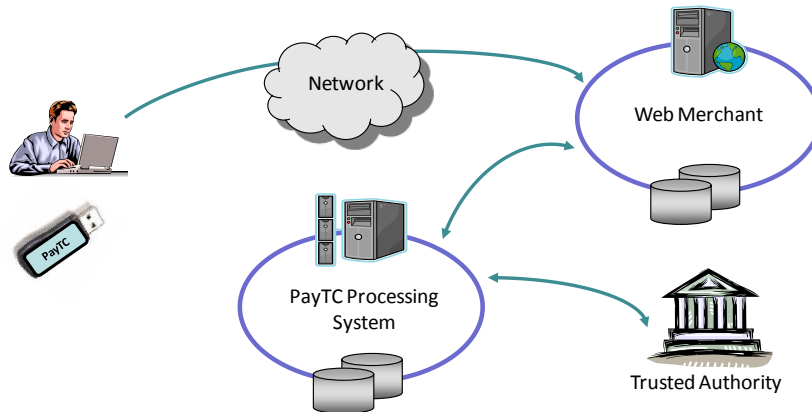
³ Patent pending: 60/952,054 US Patent and Trademark Office

TCCOPS end-to-end security features:

TCCOPS is a holistic approach to online credit or debit card security processing and further enhances the security of the online credit or debit card transaction by providing the following end-to-end security features:

Secure purchasing chain

- The contents of the PayTC™ data package can not be unencrypted by the merchant but only a trusted authority in the purchasing chain. This approach enforces the “need to know” paradigm: credit/debit card and other sensitive personal information will not be given to third parties that do not actually need this information.



Receipts

- Despite being unable to see the data inside the encrypted data package, the merchant still receives a receipt from the payment processor confirming its acceptance or denial of the transaction.

Bullet-proof security rebuilds trust

The PayTC™ validates online transactions by combining “something you know” with “something you have” and thus ensuring non-repudiation of the transaction by the consumer. By securing data so that merchants and gateways need not ever know the consumer’s personal information, TTCOPS greatly reduces the risk of identity theft and rebuilds the consumer’s trust in the online system. Credit or debit card data need never be stored in third part systems.

Ease of use makes for easy adoption

Solving the identity validation problem and greatly enhancing the consumer’s trust is only part of the business proposition of TCCOPS. The key to ready adoption is ease of use. As a USB device, the PayTC™ is readily understood by any computer literate consumer, is portable and simple to distribute. The complex technology underlying encryption, digital signatures, and closed loop data transmission is completely hidden from the consumer through the use of an easy-to-use interface on the merchant or transaction gateway web site. Furthermore, the consumer need only ever type the PayTC™ password; ***there is no need to ever type in a credit or debit card number online again.***

Conclusion

The growth of e-commerce is being stifled by concerns over identity theft and the increasing monetary losses of merchants and banks. TTCOPS is an end-to-end system that protects personal information and enables non-repudiation of online transactions with a secure, easy-to-use solution that can be readily accepted by consumers, merchants and banks.