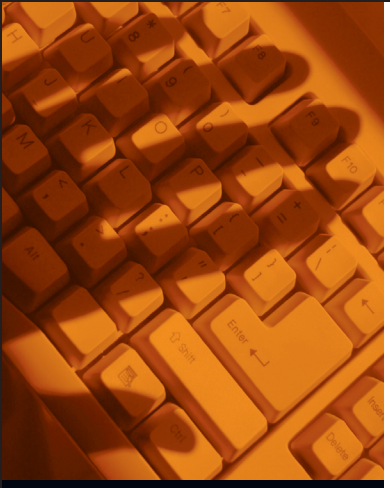

SAFETECH
Fraud and Security Solutions

Prevent Fraud and Protect Cardholder Data

BENEFITS AT A GLANCE

- **Avoid the costs of data theft resulting from fines and loss of customer confidence.**
- **Minimize lost sales and other related costs of fraud – including manual analysis and chargebacks – by detecting fraudulent activity in real time.**
- **Reduce the scope of Payment Card Industry (PCI) compliance liabilities by avoiding the processing, transmission and storage of unprotected cardholder data.**
- **Employ a transparent solution using proven technology that causes no disruption to your business or your customers.**

What are Safetech Fraud and Security Solutions?

To alleviate the risk of fraudulent transactions and stolen data, Chase Paymentech offers a full suite of fraud prevention and data encryption technologies. Safetech℠ Fraud and Security Solutions contain our premiere offerings, Safetech Encryption and Safetech Fraud Tools, as well as a variety of other proven fraud and security technologies.

Proactively Protect Cardholder Data

Safetech Encryption securely encrypts payment data as it enters the point of sale (POS), rather than encrypting it later in the payment application. This proactive approach delivers more solid data security that can help merchants reduce the scope of their PCI compliance liabilities and avoid the costs of data theft.

- Significantly reduce the PCI scope of the POS system with no need to process, transmit or store unprotected cardholder data.
- Have the assurance of deploying a solution that is more secure than software-based technology.
- Fully encrypt swiped, and manually keyed transactions.
- Experience smooth integration with most POS systems.
- Employ a transparent solution that causes absolutely no disruption to the retailer or the consumer.

Pinpoint and Stop Fraudulent Transactions

Safetech Fraud Tools can help minimize lost sales and the related costs of fraud – including manual analysis and chargebacks – while increasing sales through better order conversions. Businesses that accept card-not-present transactions (generated online or via telephone) can use Safetech Fraud Tools to:

- Detect fraud globally.
- Continuously monitor transactions.
- Automatically act on a transaction based on its fraud score.
- Employ a customizable rules engine.
- Establish customized manual review of workflows.

CHASE™ Paymentech

SAFETECH℠
Fraud and Security Solutions

Employ Advanced Anti-fraud Technology

Using some of the most advanced technology available today, Safetech Fraud Tools can help pinpoint questionable activity that can often lead to fraudulent exposure, including:

- Multiple transactions generated from a single device (e.g., computer or mobile phone)
- Transactions hidden behind proxy servers such as a prison, school, public Internet service provider, etc., to determine the true location of the consumer/fraudster
- Transactions that share common elements such as device ID, card number, address information, phone number, email address or order form attributes
- Card-testing schemes where stolen card validation is the goal
- Fraudulent activity across multiple companies over an extended period of time

Increase Sales and Customer Retention: Reduce False Positives

Companies, (on average) are rejecting 2.4 percent (U.S.) to 7.7 percent (international) of their total order volume. Of these rejected orders, 25 to 50 percent (on average) are false positives – orders that are rejected because they appear to be fraudulent, but in fact are not. The result is lost sales and often permanent loss of disgruntled customers. The advanced technology in Safetech Fraud Tools helps reduce false positives through advanced analysis methods.

Stop Unnecessary Refunds

The number of refunds issued in an attempt to prevent the occurrence of chargebacks can be equal to or greater than your actual chargeback rate. So, while you may have a relatively low occurrence of fraud-related chargebacks, you can still have an artificially high refund rate. In other words, your company may not realize that costs associated with preventing fraud are much higher than originally anticipated.

In addition to Safetech Encryption and Safetech Fraud Tools, the entire Safetech suite includes a variety of solutions to best fit your individual need or business model.

DATA POINTS

- **Retail merchants lost $139 billion in 2009 to fraud.**[**]
- **For every $100 in fraudulent transactions, merchants are paying a true cost of $310 in total losses.**[**]
- **The average cost per compromised customer record is $204.**[*]

Fraud and Security Product Options

Encryption Solutions

Safetech Encryption – Data encryption at the POS enables you to secure cardholder data during transit to Chase Paymentech's processing systems.

Tokenization – Securely stores cardholder data off-site and eliminates the need to re-key or store account data. This method also supports Payment Card Industry (PCI) compliance initiatives.

Dedicated PCI compliance team – The team works directly with Chase Paymentech customers to provide timely guidance on security and risk initiatives.

Account number masking – Technology that hides all but the last four digits of the customer's account number. It applies to both financial reports and transaction history searches initiated through our merchant data management portals.

Triple DES (3DES) encryption – Encryption technology required for PIN pads that uses three separate encryption key components to protect each transaction.

Secured terminals – Password-protected or certificate-signed payment applications residing on a terminal that protects your company by preventing malicious software downloads.

CHASE™ Paymentech

SAFETECH[SM]
Fraud and Security Solutions

Electronic Cash Register interface (ECRi) – POS software that helps protect software vendors and businesses by preventing sensitive data from being stored on cash register systems.

Chase Paymentech also utilizes a number of other encryption and security tools within our daily payment processing environment.

Fraud Solutions

Advanced, proactive anti-fraud technologies –

- IP geolocation pinpoints the location of the device, such as a computer or phone, from which a purchase is initiated.
- Device fingerprinting identifies repeat transactions from the same POS device.
- Transaction scoring shows changes in the risk profile of an order based on the real-time arrival of new data elements.
- Experiential lists identify previous negative fraud-related customer interactions, as well as the absence of fraud for good customers.
- Dynamic order linking connects potentially fraudulent orders that share little or no visible, common elements.

Fraud Filters – A web-based tool that enables sellers to block or flag suspect transactions by account number, country or payment type.

Address Verification Service (AVS) – During a transaction, a customer-supplied address and/or ZIP code is matched against payment brand information. An AVS response code then indicates whether or not the data matched.

Card Security Code (CVV2, CVC2 and CID) – A three- or four-digit number on the back of most cards that customers provide at the time of purchase to ensure the purchaser has the physical card and not just the account number.

Instant email notifications – Sends alerts on potential financial risks and exception conditions to your inbox.

Consumer authentication (Verified by Visa® and MasterCard® SecureCode™) – After clicking "buy," the cardholder is prompted to authenticate themselves with their previously selected password. This authentication information is validated by Visa or MasterCard.

Velocity Checking – Monitors the frequency of card usage during pay-at-the-pump transactions.

More Information

To learn more, visit us online at www.chasepaymentech.com.

*2010 Annual Study: U.S. Cost of a Data Breach, Ponemon Institute
**LexisNexis® True Cost of Fraud Study, 2010

CHASE™ Paymentech