



Recommendations for the Security of Internet Payments

Merchant Protect Submission



Abstract:

Merchant Protect supports an open regulatory framework, based upon minimum expectation standards, in order to foster competition and innovation in security of payments. This response addresses the proposed recommendations as they apply to authentication of transactions, such that the ECB adopts a technology agnostic best practice for online, mobile and remote payments. Merchant Protect is a fully compliant authentication system that meets or exceeds the ECB's requirements as set forth in the draft recommendations. Merchant Protect is ready for commercial deployment subject to service agreements with PSP's.

Web: <http://www.merchantprotect.com.au>

Email: security@merchantprotect.com.au

Authored by: EurIng N J (John) Karantzis & Scott W Minehane for **Merchant Protect**. Merchant Protect is a trading name of Indian Pacific Media Ltd, a company incorporated in the British Virgin Isles.

Transparency Register Identification Number 81284438347-16

20th June 2012 (Revision 1)

Introduction

Indian Pacific Media Ltd¹, (IP Media) welcomes the opportunity to respond to the European Central Bank's (ECB) 'Recommendations for the Security of Internet Payments'.

IP Media is generally highly supportive of the ECB's recommendations, and in particular the technology agnostic approach to foster competition and innovation.

IP Media owns a software based authentication system described by patent application PCT/AU2011/000377 and Australian Innovation Patent AU 201000533 A4 (Granted & Certified), which is marketed under the registered trade mark 'Merchant Protect'.²

Merchant Protect is a two-factor authentication one time password (2FA OTP) system for securing card not present (CNP) transactions. It does not require any pre-enrolment of card, cardholder, issuer, or acquirer, and it is deployed under a Software as a Service (SaaS) model. Merchant Protect operates by creating an OTP as part of the actual transaction process using existing transaction clearing infrastructure. The OTP is retrieved from an secure area by the cardholder via customer facing banking systems. These online or telephone banking systems are as currently deployed by issuing financial institutions, and they present a familiar, trusted and pre-existing interface for cardholders from which to access the OTP.

Merchant Protect is inherently and natively compatible with all credit and stored value cards issued globally by any issuing financial institution, card association network, and/or scheme, thus mitigating fraud migration and obviating the need for pre-enrolment. It is deployed by a single point integration, either by the merchant or their Payment Service Provider (PSP).

Merchant Protect does not require disclosure of, nor store, any personally identifiable information (PII). Data is devalued within the process by using anonymous references relating only to a merchant identifier and actual order number, along with an arbitrary transaction reference. At no stage are cardholders required to 'sign up' or provide personal data, nor is card specific information requested or stored by the system, diminishing the likelihood and consequence of any security breaches. As such, it is a system which is able to

¹ Indian Pacific Media Ltd is a company registered in the BVI with company number 667231

² Australian Registered Trade Mark 1405887 & 1405888

engender a high degree of confidence in online transactions by all stakeholders including banks, merchants, and consumers.

A full description of Merchant Protect is included in the Appendix, noting that Merchant Protect has several modes of operation:

- A) As a Standalone 2FA OTP authentication system in its own right
- B) As a second factor augmentation to legacy first factor (1FA) 3-D Secure systems
- C) As a collaborative technology to 3-D Secure to provide authentication on non-enrolled cards

IP Media contends that its Merchant Protect system meets or exceeds the ECB's recommendations in principle and has provided its comments in support of recommendations which are technology neutral or agnostic, whilst satisfying the intent of the 'Guiding Principles'.

General Part

IP Media is supportive of strong authentication, or two factor (2FA) as it is also known, for remote, mobile, and internet payments.

IP Media is also supportive of the technology agnostic approach adopted by the ECB, and the 'minimum expectation' approach adopted.

Innovation and competition in internet payments will be further facilitated under conditions where new market entrants can develop new technologies to known and well understood expectations, as is proposed by the ECB.

The proposed liability shift mechanism is of critical importance to foster innovation and competition. This is because any new technology is currently disadvantaged by the inaccessibility of liability shift that is currently limited and provided for as part of private scheme arrangements and agreements governing card not present transactions.

Whilst not specifically raised within these recommendations, pricing for any authentication service should be **unbundled** from the card payment scheme acquiring interchange fees³ to allow for transparency and enhanced competition in the area. The incumbent technology, 3-D Secure, is offered to merchants under a rebate against fee scheme, and is patented and owned by the largest of the card payment schemes. An ECB requirement for the unbundling of such services and pricing would be consistent with European competition law (including *inter alia* Article 102 of the Treaty on the Functioning of the European Union (TEFU)⁴ and relevant case law including decisions in the Microsoft cases⁵). Likewise, it would be in keeping with European Commission practice in promoting competition in both the telecommunications and electricity sectors.

Our understanding is that the card associations' claim that the rebate has been offered to encourage take up of the 3D Secure system. If that is the rationale, then the rebate is no longer required for that purpose once the ECB's recommendations mandate the use of authentication.

Our recommendation to the ECB is that it considers either;

- i) Authentication services are charged on a fee per service basis, and rebates factored into acquiring interchange fees as the base fees for the SEPA once authentication is mandated or,
- ii) The rebates are available to acquirers and merchants when using **any authentication service** that meets the ECB's recommendations⁶ or,
- iii) Any other alternative that fosters competition and factors the market dominance and power of the card associations.

³ For typical interchange fees and the rebate applicable to SecureCode as the Universal Cardholder Authentication Field (UCAF) see <http://www.mastercard.com/us/company/en/whatwedo/interchange/Intra-EEA.html>

⁴ Refer to <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12008E102:EN:NOT>

⁵ See Commission Decision of 24 March 2004 relating to a proceeding under Article 82 of the EC Treaty (Case COMP/C-3/37.792 Microsoft), and Summary of Commission Decision of 16 December 2009 relating to a proceeding under Article 102 of the Treaty on the Functioning of the European Union and Article 54 of the EEA Agreement (Case COMP/39.530 Microsoft (Tying)), OJ, 13 Feb. 2010, C 36/7.

⁶ For example, the definition of UCAF in the Mastercard example above would need to encompass any technology that meets the ECB's recommendations.

Observation

Whilst it is accepted that 3D Secure is the incumbent technology, the reference and inclusion by the ECB of the system with descriptions within the recommendations document provides what could be considered as a *de facto* endorsement of the system by the ECB. This in turn may provide a competitive advantage to 3D Secure, and may in addition create a non-level playing field or act as barrier to entry for emerging and/or competing technologies. Whilst some references to 3D Secure by the ECB may be appropriate, we would content that removal of the specific annexes would more properly satisfy the intent of the 'Guiding Principles'.

Response to Recommendations

Merchant Protect generally meets or exceeds the majority of the recommendations, and is ***available immediately*** as an authentication service under a SaaS scheme to PSPs in the Single European Payment Area (SEPA).

IP Media acknowledges the implementation period up to 1st July 2014, and is prepared to work with national authorities should they wish to define a shorter period. A staggered approach to implementation would best benefit PSPs, cardholders, and stakeholders to ensure that integration and customer awareness is completed well before 1st July 2014.

Our responses below are limited to the recommendations that are related to IP Media's Merchant Protect authentication service.

Merchant Protect is fully compliant with the ECB's recommendations as currently drafted, subject to some minor interpretive issues.

Recommendation 1: Governance

1.1BP Merchant Protect does not store any personally identifiable information for its core authentication service. Our policy is to devalue data and use arbitrary transaction identifiers that are passed to us by any PSP.

Recommendation3 : Monitoring and Reporting

3.2KC Merchant Protect mitigates major incident occurrence by not requesting or storing PII. Data is devalued and security breaches, if they were to ever occur, would not compromise cardholder or card data.

3.3KC Merchant Protect's response log files are available to relevant law enforcement agencies upon request. The response files provide various data, including response attempts, OTP values entered, IP address, and device serial numbers (where available). However, Merchant Protect does not store PII with data, being completely anonymous. Law enforcement agencies would need to match the transaction identifier recorded by Merchant Protect with that issued and stored by the PSP in order to ascertain the identity of the cardholder.

Recommendation 4: Risk control and mitigation

4.1KC Merchant Protect complies with the 'least privileged' principle. At no stage is PII data requested or stored from cardholders. Any security breach does not therefore expose cardholders to risk of payment fraud or loss of privacy.

4.2KC Merchant Protect utilises the PSP's communication protocols to accept data if located remotely from the PSP. The preferred implementation is for Merchant Protect's authentication agent to be co-located with the PSP, behind the PSP's firewalls.

Merchant Protect's cardholder response page can be located at either (or a combination of, or all of):

- i) the merchant's website
- ii) the PSP's website
- iii) the isignthis.com website operated by Merchant Protect
- iv) by Short Message Service (SMS) response

As response data is comprised of only the merchant's name, the order number or transaction identified (allocated by merchant or PSP), and the OTP response, data entered and held by the authentication response websites is devalued.

Any “man in the middle” or fake websites posing as the authentication websites will only capture data relating to authentication of a specific transaction. This data is in turn already associated with a pre-existing order at a merchant, that comprises already selected goods or services, and a delivery destination.

4.3KC Merchant Protect provides a range of reports associated with authentication responses, patterns, and trends.

Recommendation 5: Traceability

5.1KC Transaction data associated with authentication may include internet protocol address (IP address) and device serial numbers. In some cases, authentication application software may be utilised, which in turn may be registered by issuers to particular customers.

5.2KC Merchant Protect retains log files for evidentiary purposes. The log files are generated automatically and are not available except to authorised Merchant Protect staff as read-only.

5.3KC Merchant Protect queries and analyses log files for patterns with regards to PAN, IP address and device serial numbers (where available). Log files are not available except to authorised Merchant Protect staff as read-only.

Recommendation 7: Strong Customer Authentication

7.1KC Merchant Protect can be utilised to provide strong authentication on the first of any series of recurring transactions. Automatic triggering of authentication is available should value of direct debit change from the original authenticated value.

7.2KC Merchant Protect does not encourage the storing of payment data by merchants, and neither does it store any such data itself. In the event that PSPs are to store such data on behalf of cardholders, Merchant Protect would recommend that strong authentication takes place on at least the first transaction associated with any recently changed financial instrument.

7.3KC All cards, issued by any issuer anywhere in the world under any card scheme, are automatically, technically ready upon issue to be authenticated by Merchant Protect.

Merchant Protect has two modes of operation, similar to 3-D Secure:

- i) persistent mode
- ii) risk based assessment mode

Under a persistent mode of operation, that is, where all or a very large majority of transactions are required to be authenticated, customers would necessarily be advised that transactions are to be subjected to an authentication process. The customers could then either proceed with the transactions, or elect not to.

Under a risk based assessment mode, a risk assessment similar to that proposed by Mastercard for 3-D Secure⁷, only a small percentage of transactions would be selected for authentication. Risk assessment occurs at time of transaction.

Under both modes of operation, the customer consent will be by means of positive selection of a 'tick box' at time of transaction at the merchant's payment page (on a transactional basis), rather than at the time of card issue.

7.4KC Merchant Protect can operate in tandem with 3-D Secure. This may be of particular benefit to merchants that operate within and outside the Single European Payment Area (SEPA) and yet offer their products and services globally, as 3-D Secure is somewhat geographically restricted. This is because it relies upon registration of cards by the cardholder if their issuer participates in 3-D Secure. As the overall global adoption rate of 3-D Secure remains very low, Merchant Protect can be utilised to authenticate cards that 3-D Secure is not able to authenticate.

7.5KC PSPs do not need to change any feature of their communications interface with their merchants in order for their merchants to support strong authentication. Merchant Protect utilises the existing PSP software, communications protocols, and handshakes, and requires only one additional new status flag to be incorporated by the merchant.

The new status flag relates to whether the authentication has passed, failed, or is pending. This single point merchant integration provides coverage for all cards issued under any

⁷ See http://www.mastercard.com/us/merchant/pdf/rba_secure_code_HR.pdf

scheme anywhere in the world, and requires an absolute minimum of modifications to the communications between the PSP and merchant.

7.6KC Merchant Protect fully supports the concept of liability shift in conjunction with strong customer authentication that complies with these recommendations.

7.7KC Merchant Protect would encourage the ECB to be consistent in its treatment of eWallet providers and merchants generally when accepting internet payments. eWallet solution providers have access to suitable technologies (including 3-D Secure, Merchant Protect, and others) such that all transactions can be subjected to strong authentication. The use of strong authentication on only the first transaction creates the potential of a security gap and possible fraud for subsequent transactions if the eWallet account is compromised. Merchant Protect recommends that the ECB reconsider its proposed exemptions and require strong authentication consistently for all remote, mobile, and internet transactions, otherwise there is a possibility that the loophole will be 'gamed' by various providers in order to avoid or minimize ECB regulation.

7.1BP Merchant Protect can be enabled and integrated at the merchant (on a merchant by merchant basis if need be), rather than the PSP. This allows merchants the option to utilise alternative authentication techniques to those of the PSP, should the PSP not have enabled Merchant Protect. It is advantageous for PSPs to support Merchant Protect as this provides an aggregated, alternative authentication service for all merchants utilising any particular PSP.

7.2BP Merchant Protect natively authenticates all cards from any issuer via a single integration at the PSP or merchant. All card associations/schemes such as AMEX/CarteBlue/Discover/Eurocard/JCB/Mastercard/Visa are automatically encompassed within the Merchant Protect authentication process. Merchant Protect can also be used for debit and prepaid cards, stored value cards, and "virtual" cards that have made a recent appearance in the CNP payment environment. It is preferred that upon issue of card that it is linked to the customer's internet or telephone banking service.

Recommendation 8: Enrolment for and Provision of strong authentication tools

8.1KC [cards] Merchant Protect does not strictly require customer pre-registration of cards for cards to be technically enabled for future authentication. We would discourage registration of cards independent of the authentication process as this provides an opportunity for a potential security breach.

Merchant Protect can accommodate a preregistration process that incorporates a sign up process if it is deemed necessary by the PSP or the ECB. However, one of Merchant Protect's key attributes is that it does not require pre-sign up and does not store PII, thus reducing the risks associated with security breaches.

In the event that pre-registration is mandatory then Merchant Protect can allow for pre-registration of core customer details linked to the card's Primary Account Number (PAN) (i.e., the first 6 and last 3 or 4 digits), which becomes active upon the first successful authentication that corresponds to PAN and core customer details. Registration may include a mobile telephone number for transmission of SMS notifications, consistent with the requirements of 13.2BP.

Merchant Protect only utilises safe and trusted environments such as the customer's internet banking account for access to and retrieval of the dynamic OTP.

8.2KC There is no strict requirement for cardholders to pre-enroll in order to be technically enabled for authentication under the Merchant Protect process. We would encourage issuers to make their customers aware that there is more than one authentication process that may be in use by PSPs and/or merchants, and, where possible, to nominate authentication services that meet these guidelines.

In this regard, it would also assist innovation, new market entrants, and competition if the ECB were to publish compliant authentication services, such that PSPs, merchants, and cardholders may all be made aware of the various options.

Recommendation 9: Log in Attempts

9.1KC Access to the OTP generated by Merchant Protect is via the cardholder accessing their internet banking, telephone banking, or other appropriate means of accessing their credit card account.

SEPA utilises real time banking systems, which in turn allows near real time access by cardholders to their linked online banking facilities and thus retrieval of the OTPs and authentication via the Merchant Protect process. Many non SEPA jurisdictions do not have real time transaction processing for the purposes of updating internet banking, and rely upon overnight updates.

In our particular case, where the OTP's are retrieved from a secure environment, we advise that the OTPs ought to expire after 48 hours after issue, in order to allow cardholders (who might not necessarily be within the SEPA) to make contact with their issuing bank via internet or telephone banking. This in no way impacts the security of the system, as security relies upon the cardholder being able to access the associated account via the issuing institution's internet or telephone banking, and this time period accommodates cardholders globally irrespective of the sophistication of their Issuer. Such flexibility is likely to be required by merchants located in SEPA but offering their products and services into a global market.

Except in the case of full identity theft and compromise, accessing the Merchant Protect generated OTP would not be possible, as access is only possible after accessing the relevant account.

In the case of physically issued cards, it should be noted that all cardholders have access to the OTPs in real time from their issuer by either internet banking and/or telephone banking, and/or contacting their financial institution utilising the contact details provided to them by the issuer. Online and virtual (or cardless) systems inherently have online access.

Merchant Protect thus provides global coverage for all issued cards with the benefit of mitigating fraud migration.

9.2KC Merchant Protect is configurable by each PSP (or merchant) as to the allowable number of response attempts in total or within any defined period.

Recommendation 10: Transaction Monitoring and authorisation

10.1KC Merchant Protect can be provided to PSPs and merchants with a risk based assessment (RBA) module.

The module monitors a variety of factors, including those identified by the ECB. IP address can be monitored at both time of transaction and time of authentication response.

The RBA module also accepts inputs directly from merchants such that authentication is triggered whenever:

- i) transactions exceeding a certain value
- ii) for new customers and/or for new card data
- iii) for multiple transactions in any given period by a customer or associated with a PAN
- iv) for transactions selected by the merchant for any reason (e.g., where they include a product or range of goods, or delivery postcodes)
- v) Card BIN range is outside SEPA, or from specific jurisdictions (or vice versa)

10.1BP Merchant Protect's RBA module is a real time analytic module that does not delay payment processing in any customer discernable manner.

Unlike 3-D Secure (which interrupts the sale process), Merchant Protect's authentication process is post transactional so it does not inhibit sales, thus resulting in a negligible abandonment rate. As such, it is a revenue assurance mechanism which from our current experience has been received enthusiastically by merchants and consumers alike.

10.2BP Blocks on transactions are on a case by case basis. Where authentication is not completed within a reasonable timeframe, the transaction is reversed, with no detriment to either merchant or cardholder. Merchant Protect is a positive feedback authentication process that utilises a challenge / response approach, dynamically generating an OTP which is to be retrieved from an safe and trusted source by the cardholder (e.g., their internet banking).

Merchant Protect is based on the philosophy that all transactions can be authenticated and processes the transactions via the pre-existing authorisation cycle as determined by each card payment scheme. In the event that authentication does not take place within a predefined period of time, the transaction authorisation does not proceed to settlement, and the merchant is advised that authentication did not take place (and thus not to provide any goods or services). This approach maximises potential revenue for online merchants and

minimizes disruption and revenue leakage, whilst also resulting in a negligible abandonment rate.

Recommendation 11: Protection of Sensitive Data

11.1KC Merchant Protect does not request nor store PII. All data is stored using anonymous transaction references that are arbitrarily assigned by either merchant or PSP. Data is thus devalued as it does not directly correspond to PII nor to card details, and cannot be utilised in any way for subsequent fraudulent activities.

Recommendation 13: Notifications, Setting of Limits

13.1BP This functionality could be provided within the Merchant Protect authentication module, in conjunction with 8.1KC [cards] sign up facility.

13.2BP This functionality could be provided within the Merchant Protect authentication module, in conjunction with 8.1KC [cards] sign up facility. Merchant Protect accommodates response from cardholders via SMS or direct entry to secure web pages per 4.2KC above.

13.3BP This functionality could be provided within the Merchant Protect authentication module, in conjunction with 8.1KC [cards] sign up facility. Merchant Protect accommodates bespoke authentication triggers as outlined in 10.1KC above. This functionality could be provided within the Merchant Protect authentication module if required by PSPs.

Appendix A – Merchant Protect Technology.

We support the ECB's initiative to foster a technology neutral approach whilst adopting a minimum performance expectation standard for authentication and internet payments generally. This approach will allow innovation in authentication techniques and foster competition within SEPA.

This establishment of a regulated framework and minimum expectation criteria will provide a pathway to development and certification of new technologies. Given the tremendous growth of online transactions (in respect of which many European countries are lagging global market leaders), future near field communications ('NFC') payment and similar, it is important that a range of quality authentication innovations are available to European actors such as banks, merchants, and consumers. This is important to position the SEPA as the preferred location for both establishment of new online businesses and for existing European merchants and suppliers to offer their goods and services globally online.

Timeliness to market is also a critical factor for any emerging antifraud tool, in order for e-commerce to stay ahead of fraud. The present market arrangements being unsatisfactory in this regard, due to the variety of participants that are required to be involved.

Whilst the SEPA SCF aims to provide an innovative and competitive environment, the market power of the card payment schemes makes entry of new solutions difficult unless adopted by one or more of these payment schemes. Merchants, who are the market participants most affected by fraud, have little choice other than to adopt the technical solutions put forward by the card associations, even if alternative solutions exist that suit their requirements better. Consumers also have little option as to the protection that they are provided, however, consumer protections do exist.

The current incumbent technology is Visa's 3-D Secure⁸, which has been implemented as a single factor authentication (1FA) process in the majority of cases. This method has been

⁸ 3D-Secure is a patented (by Visa Inc.) security oriented internet protocol aimed at initiating customer authentication for internet card transactions. The name "3D" comes from the fact that there are 3 domains: one between the cardholder and the merchant, one between the merchant and its card transaction acquiring financial institution and a new one between the cardholder and his card issuing financial institution allowing the latter to authenticate his cardholder directly.

licensed by American Express, Mastercard Worldwide, and JCB and branded as SafeKey, SecureCode, and J/Secure respectively.

Visa Inc. is also the dominant player in the card network market, and the owner of CyberSource, which is the world's largest payment gateway and also a significant provider of antifraud tools. Whilst we perceive no conflict in interest in Visa Inc. seeking to mitigate risk and fraud in general, it may be necessary from a public policy perspective to facilitate introduction of competition and innovation in the authentication field such that a single market actor is not dominant in all market segments.

Authentication and liability shift is currently linked to Visa's patented 3-D Secure solution by means of contractual agreements between cardholders, financial institutions, card associations, and merchants. Whilst this has fostered the adoption of 3-D Secure, it is arguably unlikely to allow new – and perhaps better- techniques to emerge, as new market entrants will not have the market power and influence to negotiate liability shift on a mass scale through private agreements. Innovation and new techniques are more likely to develop under the ECB's minimum performance expectations consistent with the recommendations, with liability shift assured by regulation, rather than through private agreements. Such mechanisms also provide European merchants and consumers with surety regarding minimum standard of security and protection which is likely to foster online and other transactions.

3-D Secure does not provide global protection, as many financial institutions have not 'opted in' elsewhere outside of SEPA, creating a security 'gap' and an acknowledged migration of fraud. Where an issuing financial institution has not 'opted in', then all of its issued cards cannot be authenticated by 3-D Secure. As a result of this, EU based global eWallet and eCommerce operators will need to use alternative technologies to 3-D Secure in order to be provided protection for cards that cannot be enrolled such as those issued outside of SEPA and EU. As online merchants and other services proliferate globally, this 'gap' provides additional risks for merchants and consumers alike which is expanded upon below.

We also note that 1FA authentication with static passwords is susceptible to hacking⁹, and we again are supportive of the ECB's requirement for 2FA (or strong) authentication. Merchant Protect supports the migration of authentication standards to 2FA or better for e-payments and m-payments for remote payments. Two factor authentication (2FA), using one time passwords, is now already established as the standard in online transactional banking and is becoming an option as part of the 3-D Secure process.

Whilst 3-D Secure has many merits, Merchant Protect would contend that it also has some significant drawbacks, including;

- Globally, it affords protection only where issuing financial institutions are enrolled
- Cardholders must enrol in advance of completing a transaction
- Cardholders are only able to enrol if their issuing financial institution has enrolled
- Costly technical integration is required between the merchant, their acquiring financial institution, and the card issuing financial institution, that is the 3 Domains, in addition to the card processing /authorisation process
- Separate integration is generally required for each of the card association's networks, that is, each of Visa, Mastercard, and American Express
- Communication and data links are complex, resulting in a lower fault tolerance than the processing/authorisation/ settlement networks, and ultimately technical 'drop outs' and failures
- Sales abandonment rate has historically been high and frustrated eCommerce merchants. This is because authentication is required to occur before the sales process is concluded (i.e., prior to accepting payment), and customers are required to take 'extra key strokes or clicks', which is a known impediment to online sales. Abandonment occurs for a variety of reasons, including the "pre" transactional nature of 3-D Secure and its technical complexity.
- As of June 2011, Mastercard Worldwide recommended use of Risk Based Assessment in order to reduce abandonment rates and lost revenues by merchants¹⁰

⁹ See European Payment Council's resolution "Preventing Card Fraud in a Mature EMV Environment".

¹⁰ See [Mastercard Worldwide, Risk Based Assessment, http://www.mastercard.com/us/merchant/pdf/rba_secure_code_HR.pdf](http://www.mastercard.com/us/merchant/pdf/rba_secure_code_HR.pdf)

Fraud migration has been identified as a major issue by Europol¹¹, with card not present transactions representing the majority of fraud perpetrated. In approximate terms, CNP transactions account for about 25% of overall revenues but simultaneously account for about 50% of all fraud. Thus, they are 3-4 times more likely to be fraudulent than card present transactions

We consider the pre-enrolment requirement for the 3 domains as a weakness in the 3-D Secure method. As 3-D Secure is an 'opt in' in most other jurisdictions, it unfortunately encourages fraud to migrate to regions where 3-D Secure is not widely implemented. This means that European cardholders are exposed if their cards are fraudulently presented in other regions.

3-D Secure does not and cannot provide authentication for the entire global cards universe, without active participation and 'opt in' by all issuing financial institutions, acquiring financial institutions, respective merchants, and cardholders. Whilst the SEPA has a high participation rate with regard to 3-D Secure, European based ecommerce operators / merchants who use SEPA acquiring institutions are exposed to potential fraud and CNP liability when transacting with customers whose cards have been issued outside of the SEPA, and/or whose issuing financial institution is not 3-D enrolled. Ideally, pre-enrolment requirements by authentication methods should be minimised to as few actors (domains) as possible, in order to increase the number of cards that can be protected by any particular authentication method. Authentication methods should neither rely on 'opt in' such as is the case with 3-D Secure, nor allow 'opt out' for any cards.

In many markets where 3D Secure has a low adoption rate, such as the US, there is very little knowledge about 3-D Secure amongst cardholders. This has created an opportunity for fraudsters where they "phish" cardholder information (or take over an existing account) and sign up on behalf of the cardholder. They then are able to use the 3-D Secure system to safely conduct fraud.

Merchant Protect overcomes the above issues associated with 3-D Secure, and provides dynamic 2FA ***across the entire credit card universe*** without the need for ***pre-enrolment*** of

¹¹ [Europol, EU Organised Crime Assessment 2011, https://www.europol.europa.eu/sites/default/files/publications/octa2011.pdf](https://www.europol.europa.eu/sites/default/files/publications/octa2011.pdf)

the cardholder, issuing financial institution, or the acquiring financial institution. Merchant Protect can be implemented by agreement with either the PSP or the merchant, and does not require issuer, card network or acquirer participation.

In contrast, '3-D Secure' actually requires five entities to participate, being 1) the cardholder, 2) the merchant, 3) the acquirer, 4) the issuer, and 5) the card network.

Merchant Protect contends that this is not best practice for a fraud prevention mechanism, as if even one of the 5 entities does not participate, there is no way for the solution to work. Additionally, the complexity of interlinks does not lend itself to a fault tolerant solution, nor facilitate ease of integration. Serious questions need to be asked whether such a system can scale to and provide a very high level of connectivity when authentication becomes mandatory.

Merchant Protect's method inherently allows for each and every card, anywhere, to be authenticated without pre-enrolment of any type by any party.

The Merchant Protect method is premised upon providing positive feedback to the merchant regarding the authenticity of a transaction, by generation of a one-time password (OTP) within the existing authorisation and settlement cycle of each transaction.

The process then requires the customer to retrieve the dynamic OTP within a reasonable timeframe from their issuing financial institution, and provide it to the Merchant Protect authentication agent. The authentication agent then notifies the merchant upon successful response from the cardholder.

The process leverages the existing online transactional banking facilities that the customer has in place, and the associated 1FA or 2FA authentication.¹²

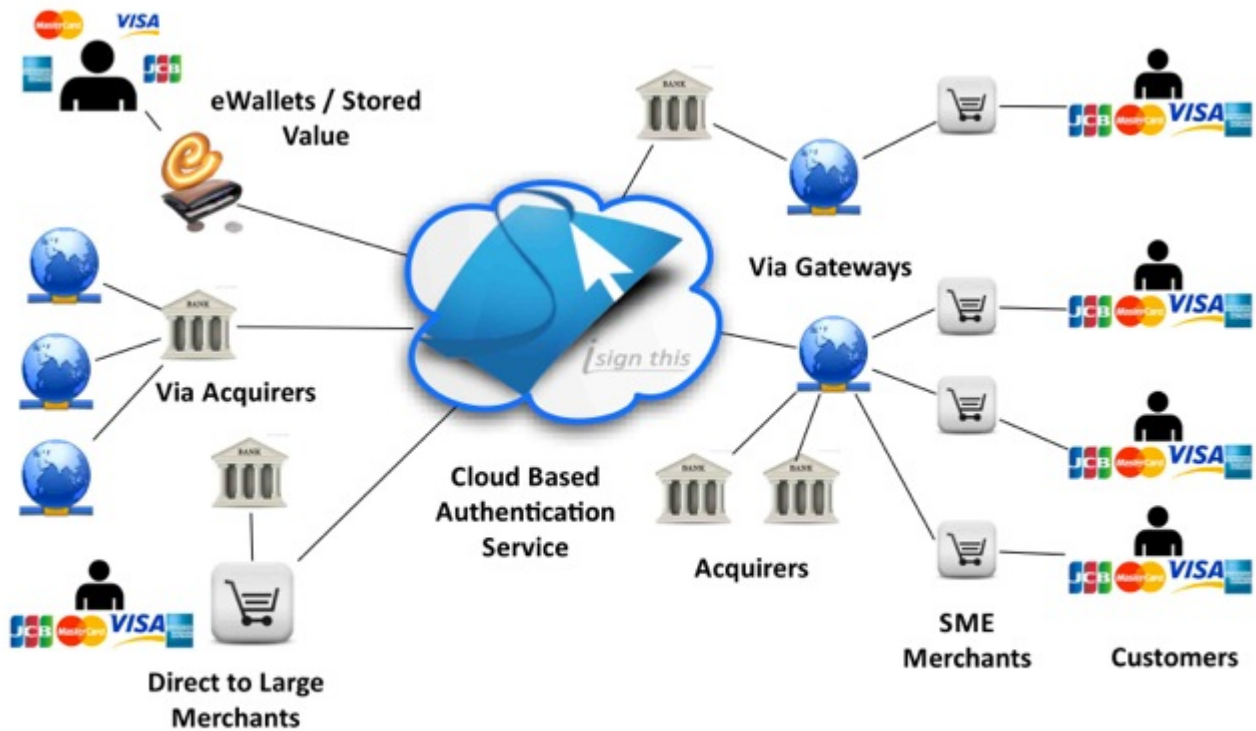
In contrast to 3-D Secure, Merchant Protect is a 2FA or 3FA process with the following attributes, which have significant benefits for European banks, merchants and consumers:

- Authenticates any card, anywhere, without pre-enrolment. Every card and card type is included automatically as the default condition.

¹² Refer Australian Innovation Patent AU [201000533 A4](http://pericles.ipaustralia.gov.au/ols/auspat/applicationDetails.do?applicationNo=2010100533),
<http://pericles.ipaustralia.gov.au/ols/auspat/applicationDetails.do?applicationNo=2010100533>

- Generates real time OTP 'in band' as part of credit card processing/ authorisation / settlement process, by innovative use of features of the transaction payment process itself.
- Extremely low cost to implement, requiring only single point integration at a point in the transaction network between merchant and pre-acquiring financial institution.
- No new physical device or deployment is necessary.
- Single integration for all card types (AMEX/CB/DISCOVER/JCB/MC/VISA).
- Cloud based with choice of integration: merchant-by-merchant, or aggregate by gateway or by acquiring financial institution or combinations.
- Provides authentication for the entire global credit card universe without the requirement for card scheme, acquiring financial institution, issuing financial institution participation.
- Easy to integrate with smartphones and online banking
- No involvement or integration required by card scheme, acquiring financial institution, or issuing financial institution. No ability to 'opt out', and no requirement to 'opt in'.
- Intuitive for cardholder. Relies upon customer's pre-existing relationship and access to their issuing financial institution.
- No Personally Identifiable Information (PII) is requested or stored at any time, so not subject to "phishing" nor database security breaches.
- Low user impact / intuitive. User is incentivised to authenticate as it's post transactional
- No impediment to sale / very low abandonment rate due to post transactional nature
- No change to transaction network software, protocols or infrastructure required.
- High technical fault tolerance, as it utilizes the pre-existing transaction settlement and clearing networks without any change to those networks.
- Global solution for automated cross border / jurisdiction / currency transaction authentication¹³
- Can be used as 2FA for 3-D Secure systems, and/or authenticate non enrolled cards

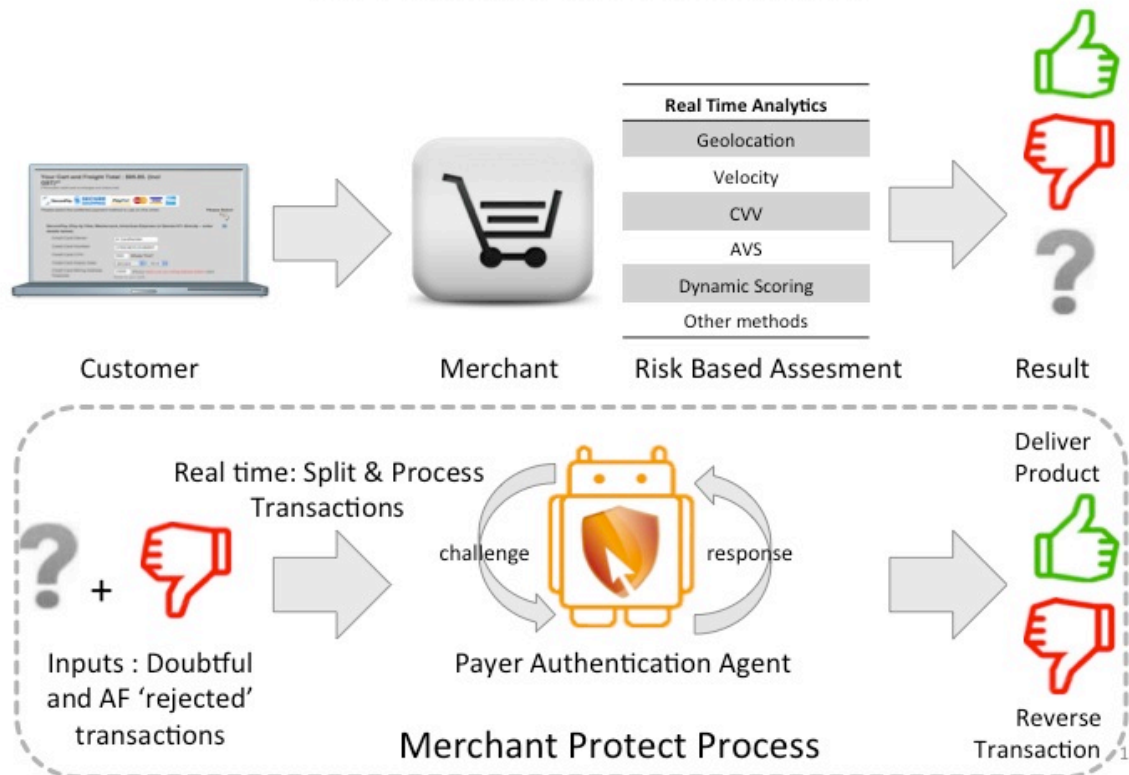
¹³ [Refer to PCT application PCT /AU2011/000377,
http://www.wipo.int/patentscope/search/en/detail.jsf?docid=WO2011120098&recNum=1&docAn=AU2011000377&queryString=FP:\(WO/2011/120098\)&maxRec=1](http://www.wipo.int/patentscope/search/en/detail.jsf?docid=WO2011120098&recNum=1&docAn=AU2011000377&queryString=FP:(WO/2011/120098)&maxRec=1)



Merchant Protect offers a variety of integration and aggregation points

Figure: A cloud based solution open to merchants, eWallets, gateways and financial institutions. Solution is also open as a second factor for 3-D Secure, or where 3-D Secure cannot authenticate.

Merchant Protect Process



The Merchant Protect Process¹⁴

1. Using a Risk Based Assessment method; **Identify** suspect/risky transactions in real time. This can be each transaction if necessary or nominated transactions only.
2. The Authentication Agent will **Split** (in real time) the nominated transaction into two (or more) debit charge amounts and *process these normally via gateway/acquiring financial institution*, thus generating an OTP.
3. The Authentication Agent will **Challenge** the cardholder to retrieve the OTP (2 x debit amounts) using their pre-existing telephone or online banking associated with the credit card.

The merchant will **Proceed** with delivery/fulfillment following positive customer response (authentication)

At step 2, the **two amounts sum to sale total** with the first of the 'split' debit amounts being generated by using a random number generator guaranteeing it is unique each time. The

¹⁴ See http://www.merchantprotect.com.au/mp_isignthis_V6.pdf

second debit charge amount is a balancing debit charge up to the sale total amount. The OTP keys are thus dynamically generated and are comprised of the transaction value itself. The process is post transactional, and cardholders would not necessarily know until after the sale has been completed and transaction authorised by their issuing financial institution if they are required to authenticate. Thus, the process does not impede sales, and results in a far lower abandonment rate, as cardholders have already completed the transaction. This is unlike 3-D Secure which is “pre” transactional, resulting in higher abandonment rates.

At step 3, only the legitimate account holder will be able to access the account and retrieve the OTP from their issuing financial institution. The process works irrespective of issuing financial institution, acquiring financial institution or cardholder involvement, jurisdiction or currency, or the level of sophistication of the issuing financial institution. Even in cases where online transactional banking and automated telephone banking is non-existent, the cardholder is able to contact their issuing financial institution using the contact details on the reverse side of their credit card, and providing that they can identify themselves, will be able to access the two debit charges.

The customer experience during authentication is thus to access their credit card account statement via a trusted and familiar means, retrieve the OTP, and then to provide the OTP along with the merchant identifier/order number to the authentication agent, without disclosing any personally identifiable information (PII) in the process. A major benefit is that no new web pages or processes have been introduced with the cardholders already familiar with the banking processes associated with their issuing institution.

At step 4, the Authentication Agent confirms the OTP matches that which it generated, and advises the merchant that positive feedback authentication has taken place. The process thus only requires the enrolment of the merchant, with integration able to be aggregated at gateways or acquiring financial institutions such that the Authentication Agent is cloud based.

Whilst minor network charges and costs may be associated with splitting transactions, the corresponding reduction in fraud rates or chargeback administration fees will more than offset any additional costs.

Implementation by merchants of the Merchant Protect system in Australia has shown that fraud attempts drop off rapidly. Authentication is typically within minutes for over 70% of transactions, and same day for over 95%.

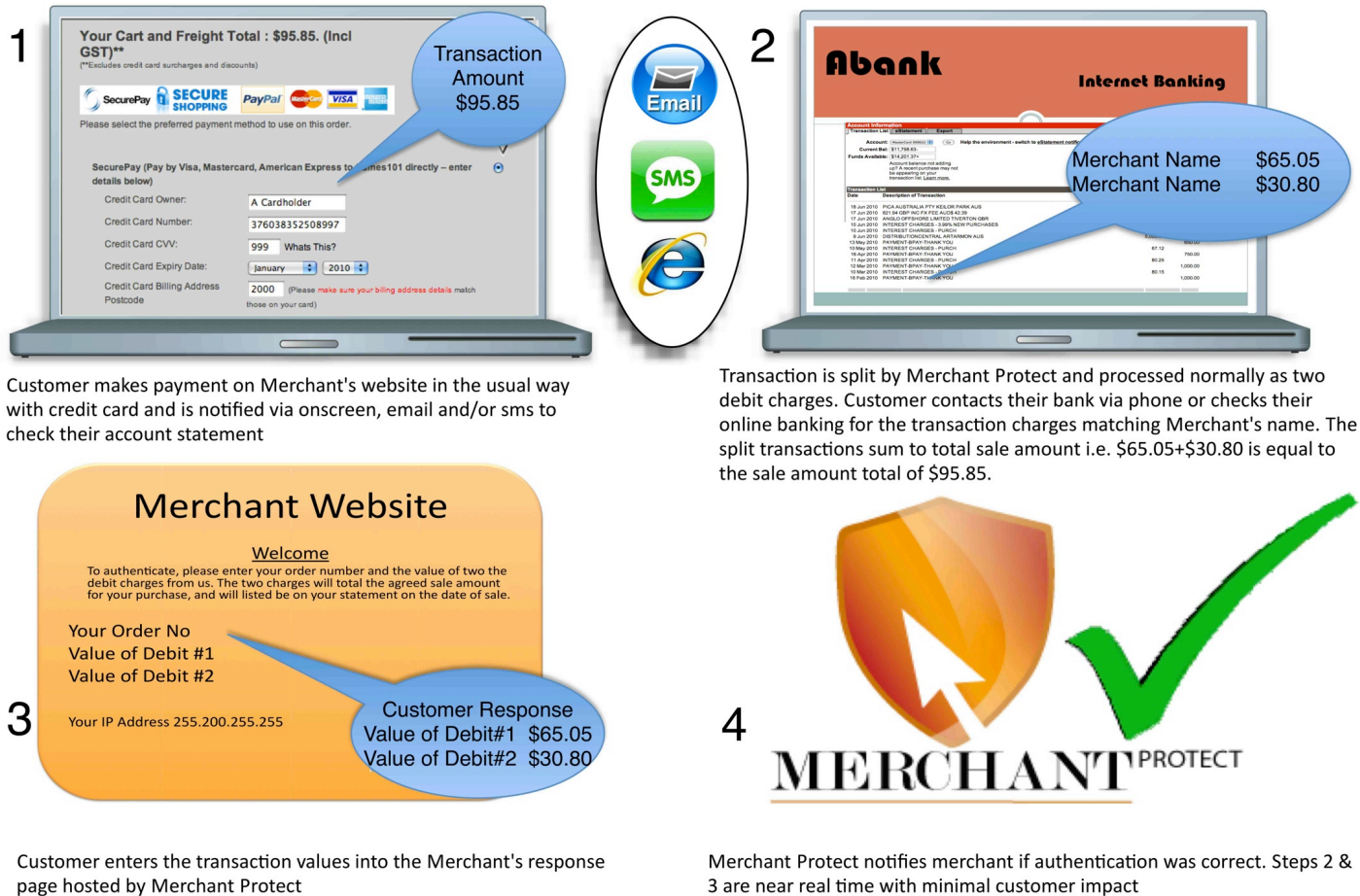


Figure: The authentication process, leveraging the customer's pre-existing relationship with their financial institution and the authentication processes already in place at such.

A further advantage of the Merchant Protect process is that it can be optionally adopted by issuing institutions, in addition to merchants, gateways, or acquiring institutions. The solution can be aggregated at processing gateways such that many merchants and many acquiring financial institutions are integrated with a single agent at the gateway.

Issuing institutions can also integrate the solution to provide customized user experience based upon the sophistication of their online transactional banking systems.

Merchant Protect meets the performance principles of the EPC resolution ‘Preventing Card Fraud in a mature EMV Environment.’

Standard Authorization Process with 3DS (1FA) Authentication

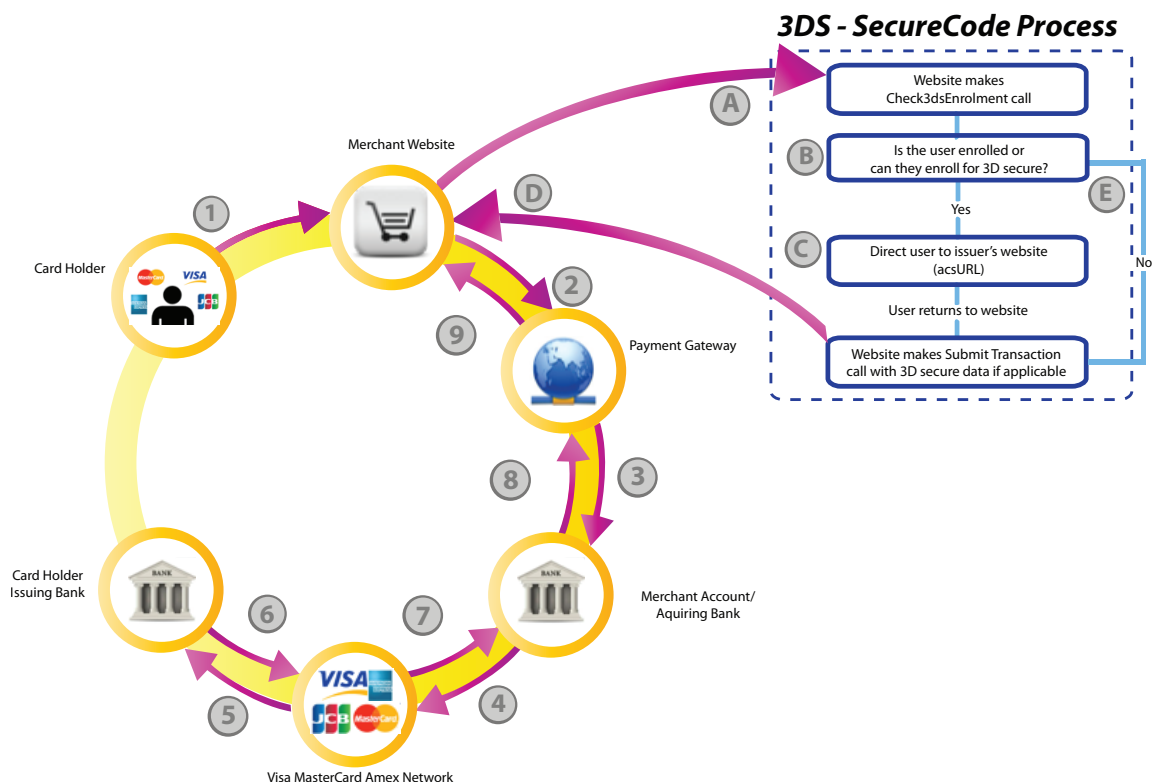



Figure: Merchant Protect is interposed in the standard authorization and settlement cycle, without changing any software protocols at merchant, gateway, acquirer, card association or issuing financial institution.



Welcome!

If you have been directed here by a merchant or service provider with whom you have recently made purchase, then please follow your merchant's instructions to retrieve the charge values, and then enter below.


Press the button below when value entry completed to authenticate your payment.

Merchant Name

Merchant Reference

Higher Charge Value

Lower Charge Value

Authentication: 

Authenticate

NB!
Your details remain anonymous, and we do not store any credit card, bank account or personal data at any time.

[HELP](#) [Merchants](#) [Security](#) [Legal & Patent](#)

Benefits (Orange Box):

- 'Anonymous' reference data unrelated to PII.
- No opportunity for hackers
- No PII requested or stored
- No preregistration or sign in

isignthis Description (Blue Box):

isignthis is a new way of authenticating online transactions when using your preferred credit card.

Authentication proves that you are the cardholder, as only the cardholder will have access to the card account via internet or phone banking. isignthis secures your online transactions, preventing fraud and protecting you.

isignthis is safe, easy and completely anonymous. It acts just like your personal signature, without asking you to disclose any personal data.

12

Figure: Customer response web page – anonymous, with no intrusive or PII data requested, nor any requirement for advance sign up.

Merchant Protect as a Second Factor Authenticator for 3D Secure

Merchant Protect can support 3-D Secure / SecureCode / SafeKey / J/Secure via two means:

1. As a strong second factor authentication method, and/or
2. As a primary authentication factor for non-enrolled cards.

SMS based second factor authentication has been widely adopted in conjunction with 3DS in order to facilitate an OTP. However, SMS authentication is not a primary authentication method for transactions, and is of no assistance when 3DS cannot authenticate a transaction due to a card not being enrolled.

In such cases, Merchant Protect can be utilised as a second factor authenticator for implementations of 3-D Secure, in lieu of SMS (or other non-primary authentication means) as the second factor. The advantage to this approach is that for non-enrolled cards that cannot be authenticated under 3-D Secure (with or without SMS), Merchant Protect can function as the primary authenticator, *allowing authentication of every card, everywhere*.

Merchants can adopt Merchant Protect independent of their acquirer and 3DS, taking advantage of Merchant Protect's ability to authenticate every card without the need for pre-enrolment. The existing security gap created by 3DS is then closed, allowing merchants to transact globally with confidence, as cardholders cannot 'opt out' of the process.

In this way, fraud migration is significantly mitigated, as Merchant Protect provides authentication of any card, anywhere, without the requirement for 'opt in' from financial institutions.

Merchant Protect could also be implemented with Risk Based Assessment, such that any 1FA 3-D Secure system may 'refer' riskier transactions to Merchant Protect as its second factor authentication. This may be for larger value transactions, transactions originating outside SEPA, high risk products, or first time transactions. Merchants, gateways, or acquiring institutions would be able to enhance their security and reduce threat of fraud, thus increasing the security within their area of operation without relying upon issuing financial institutions in other jurisdictions being enrolled in any particular program.

This then provides a competitive environment for authentication within the EU and SEPA, as merchants can elect to act independently of the card associations, or in conjunction with them, in order to achieve the desired level of security based upon the scope of their operations.

Standard Authorization Process with 3DS (1FA) Authentication

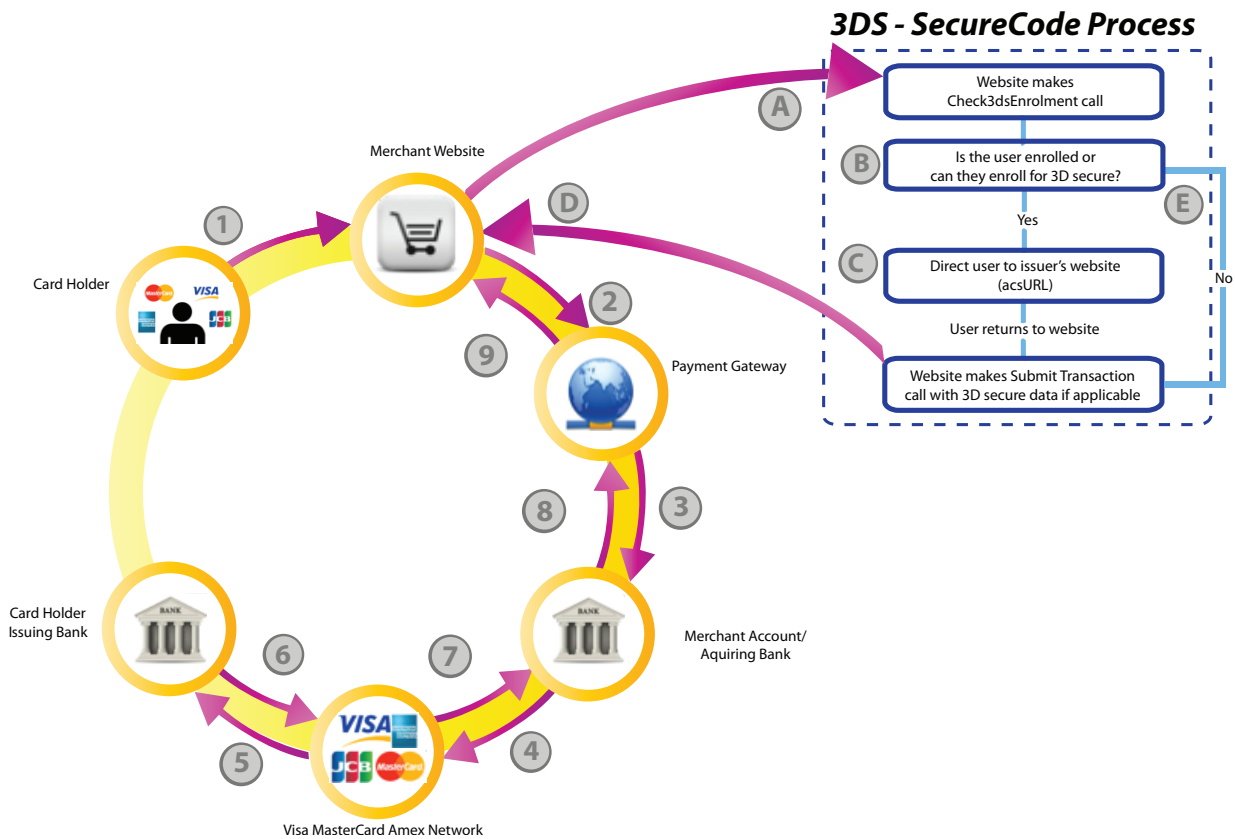


Figure: Standard 3D Secure implementation, prior to transaction being sent to gateway for processing.

Merchant Protect as Second Factor Authentication (2FA) with 3DS as First Factor Authentication (1FA)

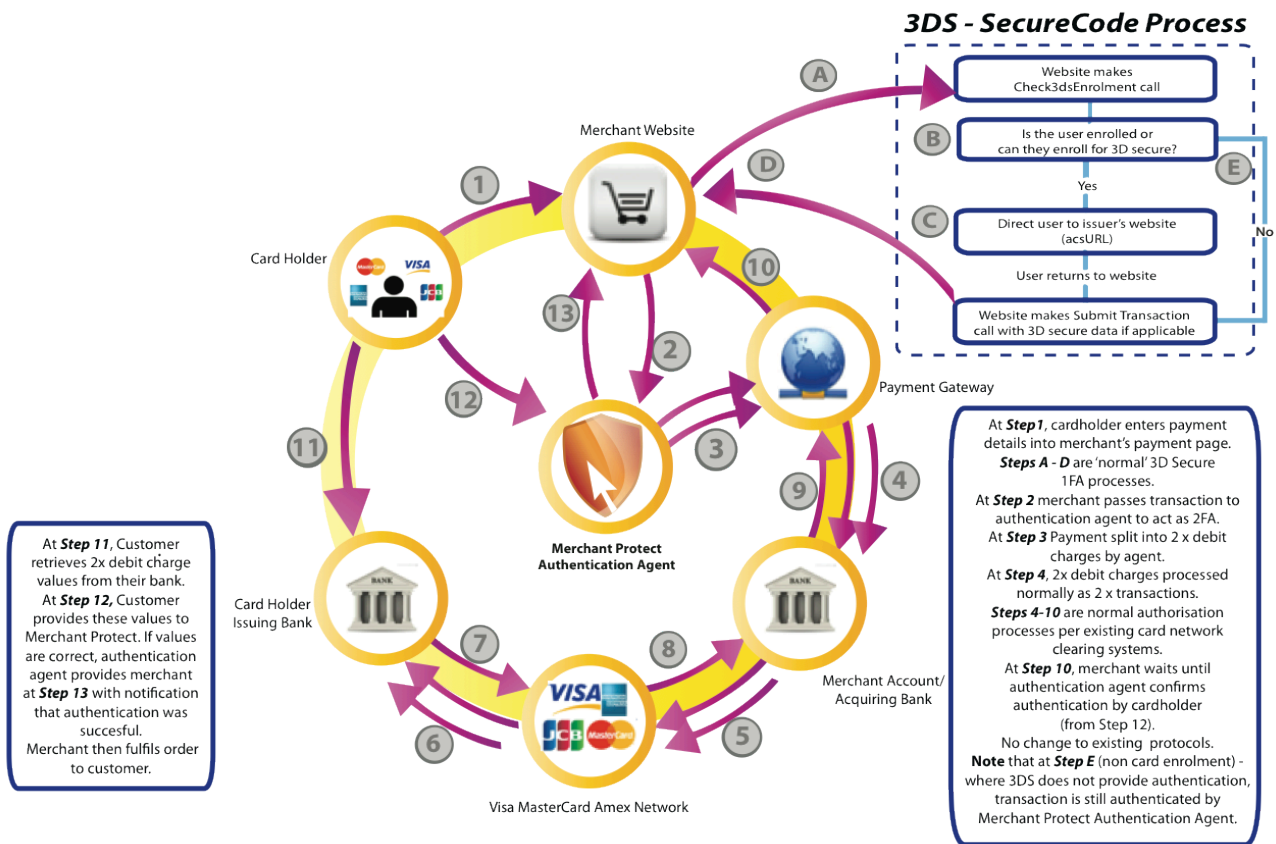


Figure: Merchant Protect as second factor authentication, providing protection and authentication where 3DS cannot.

Mobile and eWallet Advantages

- Merchant Protect is intuitive and lends itself to eWallets and mobile applications
- No mandatory pre sign ups or requests for personal identifiable information means that no such data is stored, thereby eliminating security risk.
- Credit Card PAN (first 6, last 4 numbers) can be preregistered and linked to a mobile phone in order to allow for mobile authentication applications to be built, whilst still maintaining anonymous nature of information held. This can be used as second or third factor whereby 1FA online banking transactional systems are used to retrieve the OTP.
- No dummy transactions or extensive wait periods for authentication cycle.

- Single, unified solution across all card types (Visa/MC/AMEX/JCB), leveraging existing mobile transactional banking systems.
- High technical fault tolerance due to simplified communication schemes and ability to present transactions again or 'offline' for split processing, if communication links temporarily fail.

Regulatory Environment – The Payment Services Directive (Annex 1)

IP Media's position is that continuing development of the regulatory framework is necessary to encourage innovation in the area of authentication, and to ensure that competitive technologies emerge for different applications. The ECB's recommendations, in our opinion, provide much needed clarification and support to the Payment Services Directive in this critical area.

Presently, merchants are faced with no real choice of competitive authentication technologies, as only the 3-D Secure/SecureCode/SafeKey/ J/Secure offer a liability shift at present for remote payments.

For eWallets and e-commerce with global operations, the ability to implement a 2FA system that provides a global antifraud solution whilst being afforded a 'liability shift' in the SEPA at present requires a combination of technologies in conjunction with '3-D Secure'. Merchant Protect now offers a unified, single solution as an alternative, which can be utilised on a global basis.

A secondary but nevertheless import issue is that of assessment of whether a technology meets or exceeds the performance criteria should be made by a certifying or regulatory body, such that actors with dominant market positions cannot set de facto standards, and mandate use and thus set associated costs for any particular technology. A certification process, similar to that proposed by the European Payment Council for cards and terminals, should also be implemented within SEPA for authentication methods.

The ECB should also continue to be technology neutral and avoid direct reference to any single patented technologies such as 3-D Secure, and continue to set out minimum performance expectations.

From an IP Media perspective, no market participant other than either the PSP or any individual merchant (on a case by case basis if desired) is required in order to implement our system.

All internet payments, be they m-payment or e-payment actors including eWallets, would in our view benefit from a regulatory framework that requires a minimum of 1FA for transactions up to a certain value¹⁵, and dynamic 2FA for transactions beyond that limit. Certain areas of commerce may require mandatory 2FA, particularly electronic stockbroking, online gaming, and online betting to ensure the authenticity of the customer. If a performance specification approach is mandated, then technologies may emerge to consolidate anti money laundering/anti terrorist financing (AML/ATF) and know your customer (KYC) requirements, resulting in a more efficient and simplified process.

The most appropriate mechanism is to devalue data stored on databases, wherever possible, by not linking the data to personally identifiable information (PII). Dynamic data that is linked to a single transaction also devalues the data and removes opportunity for hackers to breach databases.

Database Security

Merchant Protect does not require nor store PII, and generates an OTP. Merchant Protect cannot suffer from data breaches as its stored data is anonymous and 'one time' only, relating to a single transaction. It does not store card details, customer names, and indexes using only a transaction reference per merchant, the original euro amount, and the generated euro 'split values'. Once the cardholder responds, the response data, IP address, and other device fingerprinting data is captured to provide an evidentiary trail for each discrete authentication. All of this is anonymous and not linkable to an actual card account or person, thus not requiring a high level of data protection.

An additional benefit is that even in cases where other party's databases are breached, Merchant Protect would still be able to prevent fraud as fraudsters would not be able to authenticate cards with the details gained from database breaches.

¹⁵ To allow for NFC payments as m-payments.

Further Information

Further information regarding Merchant Protect is available at

<http://www.merchantprotect.com.au>

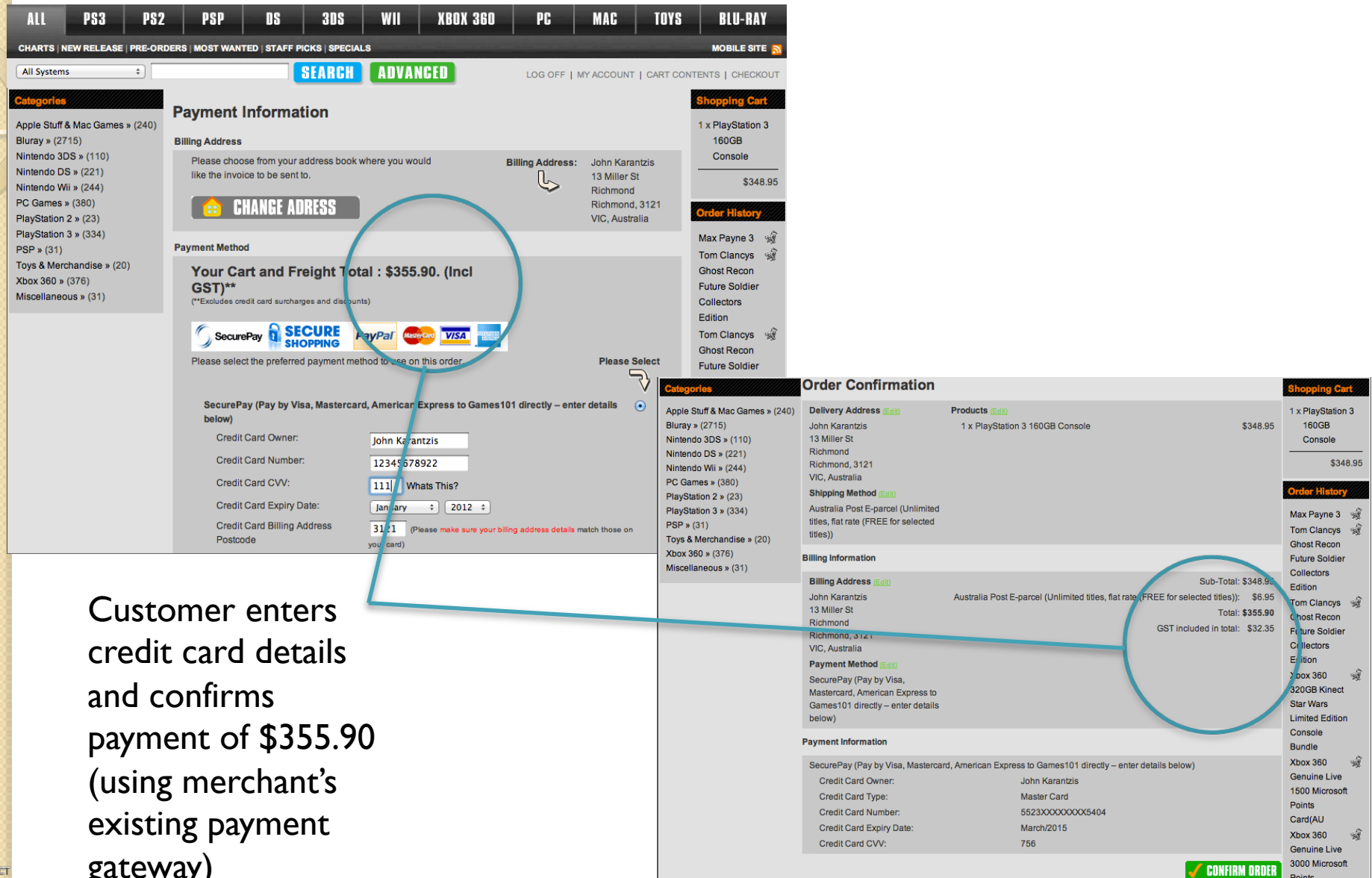
and download literature at:

http://www.merchantprotect.com.au/mp_isignthis_brochure_V6.pdf

Customer Payment/Authentication Flow Example

(4 pages)

Customer Authentication Flow 1



Payment Information

Billing Address

Please choose from your address book where you would like the invoice to be sent to.

Billing Address: John Karantzis
13 Miller St
Richmond
Richmond, 3121
VIC, Australia

CHANGE ADDRESS

Payment Method

Your Cart and Freight Total : \$355.90. (Incl GST)**
(*Excludes credit card surcharges and discounts)

SecurePay **SECURE SHOPPING** PayPal MasterCard VISA

Please select the preferred payment method to use on this order.

SecurePay (Pay by Visa, Mastercard, American Express to Games101 directly – enter details below)

Credit Card Owner: John Karantzis

Credit Card Number: 12345678922

Credit Card CVV: 1111 [Whats This?](#)

Credit Card Expiry Date: January 2012

Credit Card Billing Address Postcode: 3121 (Please make sure your billing address details match those on your card)

Shopping Cart

1 x PlayStation 3 160GB Console \$348.95

Order History

Max Payne 3
Tom Clancys Ghost Recon
Future Soldier
Collectors Edition
Tom Clancys Ghost Recon
Future Soldier

Order Confirmation

Delivery Address (Edit)

John Karantzis
13 Miller St
Richmond
Richmond, 3121
VIC, Australia

Products (Edit)

1 x PlayStation 3 160GB Console \$348.95

Shipping Method (Edit)

Australia Post E-parcel (Unlimited titles, flat rate (FREE for selected titles))

Billing Information

Billing Address (Edit)

John Karantzis
13 Miller St
Richmond
Richmond, 3121
VIC, Australia

Payment Method (Edit)

SecurePay (Pay by Visa, Mastercard, American Express to Games101 directly – enter details below)

Payment Information

SecurePay (Pay by Visa, Mastercard, American Express to Games101 directly – enter details below)

Credit Card Owner: John Karantzis

Credit Card Type: Master Card

Credit Card Number: 5523XXXXXXX5404

Credit Card Expiry Date: March/2015

Credit Card CVV: 756

Order Confirmation Summary

Sub-Total: \$348.95

Australia Post E-parcel (Unlimited titles, flat rate (FREE for selected titles)): \$6.95

Total: \$355.90

GST included in total: \$32.35

CONFIRM ORDER

Customer enters credit card details and confirms payment of \$355.90 (using merchant's existing payment gateway)



Customer Authentication Flow 2

The screenshot shows the Games101 website interface. At the top, there are navigation tabs for various gaming platforms: ALL, PS3, PS2, PSP, DS, 3DS, WII, XBOX 360, PC, MAC, TOYS, and BLU-RAY. Below these are links for CHARTS, NEW RELEASE, PRE-ORDERS, MOST WANTED, STAFF PICKS, and SPECIALS. A search bar is present with a dropdown menu set to 'All Systems' and buttons for 'SEARCH' and 'ADVANCED'. On the left, a 'Categories' sidebar lists various game genres and their item counts. The main content area is titled 'Your Order Is Pending Authentication' and explains that the user's credit card needs to be authenticated for security. It provides a three-step process: 1. Log in or call the bank to get two charges. 2. Confirm the values of these charges on the Games101 website. 3. Enter the values and select 'authenticate' in the orders section. A shopping cart on the right shows 0 items and an order history with recent purchases like 'Max Payne 3' and 'Tom Clancys Ghost Recon'.

Categories

- Apple Stuff & Mac Games » (240)
- Bluray » (2715)
- Nintendo 3DS » (110)
- Nintendo DS » (221)
- Nintendo Wii » (244)
- PC Games » (380)
- PlayStation 2 » (23)
- PlayStation 3 » (334)
- PSP » (31)
- Toys & Merchandise » (20)
- Xbox 360 » (376)
- Miscellaneous » (31)

Your Order Is Pending Authentication

You can check delivery status by logging into your account above at any time.

Thank you for your order with Games101.

For your own security and to prevent online fraud, we need to authenticate your credit card against this transaction. This is similar to signing for your goods at a physical store, as, like a signature, your authentication response will be unique.

We have emailed you detailed instructions on how to authenticate your credit card. Please note that your order will not be dispatched until you have authenticated.

You can authenticate your credit card transaction using the following quick and easy process:

Step 1
Log in or call your bank, and access your credit card account

Step 2
Confirm the value of the two charges from Games101 (values add up to your order total of \$355.90)

Step 3
Enter these values on the Games101 Website (Log in to your account, and select 'authenticate' in the orders section)

For more information (which we have also e-mailed to you), refer to the [detailed authentication instructions](#). We have sent you an email with full instructions, and will provide reminder emails at regular intervals.

You can view your order history, authenticate orders, check order status, update delivery address book and change other preferences by going to the 'My Account' page. Please direct any questions you have to Games101.

Thanks for shopping with us online!

Shopping Cart

0 Items

Order History

- Max Payne 3
- Tom Clancys Ghost Recon
- Future Soldier
- Collectors

Risk Based Assessment determines that order is to be authenticated. Customer receives on screen and email instructions to access their bank and retrieve the two values that add up to \$355.90 (order total)

The screenshot shows an email from Games101 to John Karantzis. The subject is 'Games101 Order 10527 - Authentication Required Before Dispatch'. The email explains that the order is pending authentication for security reasons. It details the three-step process: logging in to the bank to get two charges, confirming their values on the Games101 website, and then authenticating the transaction. It also mentions that the authentication process is secure and does not require disclosing personal details. The email concludes with instructions on how to contact the bank and provides transaction codes for the debit transactions on the credit card statement.

Games101 Order 10527 - Authentication Required Before Dispatch

the Games101 Wiz

Sent: Tuesday, 5 June 2012 8:46 PM

To: John Karantzis

Dear John Karantzis

At Games101 we take online security seriously, and take various steps to protect you from online fraud.

For your own security, completing the process below confirms that you are the authorised cardholder and initiated this transaction.

Our authentication process does not require you to disclose or send us any personal details, and only requires confirmation of code details that we generate and are then available from your online or telephone banking /credit card statement. Only the cardholder reasonably know these code details, and they are generated as part of the transaction you initiated with Games101.

We use Merchant Protect as our Payer Authentication system, as it is fast, does not require resubmission or store any of your personal or credit card details, and provides a log of responses for reference in case of a security breach by a fraudster on your credit card. The codes generated for this process are one time use and unique. In this way, it is as individual as your physical signature at checkout.

As the credit card holder you will have access to your account by accessing your telephone or online banking.

You can contact your bank by calling the telephone number on the reverse of your credit card. If you are using a corporate card, please email us from a company email address confirming details of the company name and delivery address.

Your credit card statement will have two transaction codes from us that look something like this:

Games101_Richmond.cd

Games101_Richmond.yz


These two debit transactions on your statement will sum to the agreed total of \$355.90 for Games101 Order No 10527. You may be able to open a new browser window, log in to your online banking in the usual way, and locate the entries within minutes depending upon your bank - otherwise, debits are processed overnight.

Upon locating the entries, we request that you log in to your Games101 account and visit https://www.games101.com.au/account_verify_order.php?order_id=10527, or follow the link to "Authenticate Payment" from your account.



Customer Authentication Flow 3

The screenshot displays the Commonwealth Bank online banking interface. The top navigation bar includes links for 'My home', 'View accounts' (highlighted with a yellow callout), 'Transfers', 'BPAY', 'Offers & apply', 'MORE', and 'INBOX'. Below this, a secondary navigation bar shows 'Transactions' (highlighted), 'Future transactions', 'Statements', and 'Account information'. The main content area is titled 'Transactions' and features a search bar with an 'Account' dropdown and a 'GO' button. Below the search bar is a table with columns: 'Nickname/Type', 'Card/Account number', 'Account balance', and 'Available funds'. The table shows one entry: 'MasterCard Diamond' with a balance of '\$1' and 'CR'. Below this table is a link to 'Show transaction search'. The 'Pending transactions' section is highlighted with a blue oval and contains a table with columns: 'Date', 'Transaction description', 'Debit', and 'Credit'. The table lists two pending transactions from 'Games 101 Richmond AUS' on 05/06/2012, with debit amounts of \$53.60 and \$302.30. On the right side of the interface, there is a 'Contact us' section with a phone icon and text: 'Call us on 13 2221, 24 hours a day, 7 days a week.' Below this is a yellow box with the text: 'Bank wherever you want. CommBank Kaching for iPhone. Download now >>'. At the bottom right, there is a 'More offers' link and an 'I want to' section with an information icon.


CommonwealthBank  My home **View accounts** Transfers BPAY Offers & apply MORE INBOX


Transactions Future transactions Statements Account information

Transactions


Account GO

Nickname/Type	Card/Account number	Account balance	Available funds
MasterCard Diamond	---	---	\$1 CR


 [Show transaction search](#)


Pending transactions 

Date	Transaction description	Debit	Credit
05/06/2012	PENDING - Games 101 Richmond AUS	\$53.60	
05/06/2012	PENDING - Games 101 Richmond AUS	\$302.30	

Contact us 
Call us on 13 2221, 24 hours a day, 7 days a week.

Bank wherever you want. CommBank Kaching for iPhone. Download now >>

 [More offers](#)

I want to 

Customer accesses their online or telephone banking and notes the two pending amounts, which sum to the order total of \$355.90



Customer Authentication Flow 4

HOME ABOUT NEWS REVIEWS TRAILERS CONTACT SIGN UP BUY GIFT CARDS

LEGO BATMAN 2 DC SUPER HEROES

ALL PS3 PS2 PSP DS 3DS WII XBOX 360 PC MAC TOYS BLU-RAY

CHARTS | NEW RELEASE | PRE-ORDERS | MOST WANTED | STAFF PICKS | SPECIALS

All Systems **SEARCH** **ADVANCED** LOG OFF | MY ACCOUNT | CART CONTENTS | CHECKOUT

Categories

- Apple Stuff & Mac Games » (240)
- Bluray » (2715)
- Nintendo 3DS » (110)
- Nintendo DS » (221)
- Nintendo Wii » (244)
- PC Games » (380)
- PlayStation 2 » (23)
- PlayStation 3 » (334)
- PSP » (31)
- Toys & Merchandise » (20)
- Xbox 360 » (376)
- Miscellaneous » (31)

Orders awaiting authentication

This order is linked to a pair of split-payment debit value transactions charged to your credit card. The two debit values have been charged in Australian dollars and when added together will sum to your exact order total shown below.

Please enter the two transaction values from your online bank statement in either Australian dollars or the currency of your card (select "other" Card Currency if not responding in Australian dollars).

Order Number: 10527 Credit card authentication status: Pending

Order Date: Tuesday 05 June, 2012	Total Order Value: \$355.90
Larger Debit Value <input type="text" value="302.30"/>	Smaller Debit Value <input type="text" value="53.60"/>
Card Currency in use <input type="text" value="Australian Dollars"/>	Card Billing Postcode <input type="text" value="3121"/>

UPDATE

Shopping Cart

0 items

Order History

- Max Payne 3
- Tom Clancys Ghost Recon
- Future Soldier

Customer enters the two values, \$302.30
And \$53.60 (=\$355.90)
Max 3 attempts. Multicurrency capable.

Upon success, customer sent confirm email and advised on screen.
If no response<>72hours, transaction reversed (can allow for manual contact)

HOME ABOUT NEWS REVIEWS TRAILERS CONTACT SIGN UP BUY GIFT CARDS

SPECIALS

ALL PS3 PS2 PSP DS 3DS WII XBOX 360 PC MAC TOYS BLU-RAY

CHARTS | NEW RELEASE | PRE-ORDERS | MOST WANTED | STAFF PICKS | SPECIALS

All Systems **SEARCH** **ADVANCED** LOG OFF | MY ACCOUNT | CART CONTENTS | CHECKOUT

Categories

- Apple Stuff & Mac Games » (240)
- Bluray » (2715)
- Nintendo 3DS » (110)
- Nintendo DS » (221)
- Nintendo Wii » (244)
- PC Games » (380)
- PlayStation 2 » (23)
- PlayStation 3 » (334)
- PSP » (31)
- Toys & Merchandise » (20)
- Xbox 360 » (376)
- Miscellaneous » (31)

Orders awaiting authentication

Transaction was authenticated successfully. Your order will now proceed.

Order has now been successfully authenticated

Games101 uses Merchant Protect as its Payer Authentication system. International Patents applicable. See www.merchantprotect.com.au

BACK

Shopping Cart

0 items

Order History

- Max Payne 3
- Tom Clancys Ghost Recon
- Future Soldier
- Collectors Edition
- Tom Clancys Ghost Recon
- Future Soldier
- Collectors Edition

