eBook

Credit Card Fraud

no company or industry is immune

ipsi

simplifying payments

Who is affected by cybercrime & fraud?

Credit card fraud affects individuals, corporations & small businesses. It is a significant problem globally and within Australia, and no company or industry is immune.

Previously major organizations with large customer bases were the cybercriminals prime focus, over the last five years this focus has shifted to include small to medium sized businesses. With issues ranging from remote hacking to ransomware and internal employee fraud.

The cost of cybercrime to the Australian economy has previously been estimated at more than $2 billion, as reported in the Identity Crime and Misuse in Australia 2013-14 Report by the Australian Government's Attorney General's Department. In 2016, the average cost of a data breach to a company was $2.51 million.

According to the Australian Cyber Security Centre's 2015 Cyber Security Survey, half of all major Australian businesses experienced at least one cyber incident in the past year, with 56% of survey respondents having increased expenditure on cyber security in the past 12 months. The increased spending primarily went towards new technical and procedural controls, obtaining vulnerability assessments and compliance audits.

The rate of fraud across Australian cards and cheques, which is measured per $1,000, increased on average by 18% year-on-year, according to the Australian Payments Clearing Association (APCA).

Financial institutions, retailers, the healthcare and education sectors, government bodies and computer software providers are all major targets for attack.

Industry figures show that there was a 64 per cent increase in the number of data breaches in the financial year 2014-15 (with sustained growth in 2016) with a spate of high-profile security attacks on companies such as Sony, eBay and Target in the United States as well as David Jones and Kmart in Australia illustrate the challenges faced across the globe.

YAHOO!

admitted that it had
a major security breach
with more than

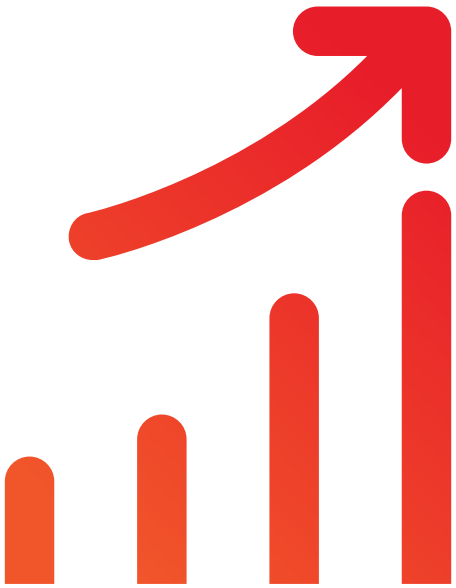
500 million

user accounts being exposed.

Worrying statistics

Payments industry data for 2016 show that fraud on Australian payment cards continues to increase in the card-not-present space, reflecting a global trend both in online card fraud and cybercrime in general.

Card fraud rates in recent years have grown from 58.8 cents to 66.8 cents for every $1,000 spent.



The majority of this increase is due to the rise in card-not-present fraud, which on Australian cards has risen 38 per cent to nearly $136.7 million, with around $47.8 million occurring overseas.

This can be partly understood by the continued and growing popularity of the use of payment cards in card-not-present environments such as the internet, mobile devices and via call centers.

According to a study of consumer payments by the Reserve Bank of Australia, the proportion of card purchases made offline, by telephone or mail order represent nearly 25 per cent of the total value of debit card purchases and about 40 per cent for credit cards.

These figures highlight a shift in spending habits and provide an insight into where fraud is occurring.

Card not present fraud increased 13% to $226.3 million up from $200.9 million in 2014, with many experts attributing this shift to improved security within card present point of sale processes.

Online fraud

As industry measures to reduce payments fraud in one area take effect (through, for example, the widespread adoption of chip technology in cards and terminals) criminals then start to focus more on fraudulent activity that is easier to perpetrate in other areas, such as online.

Card-not-present fraud is just one manifestation of the growing threat from cyber criminals experienced by governments, businesses and individuals worldwide.The online space is being targeted more widely by criminals in general, as it's easier to target remotely from overseas.

CNP fraud is the most prevalent type of fraud on Australian cards, reflecting the general increase in cybercrime. In 2015, CNP fraud accounted for

79%

of the Australian cards with counterfeit/skimming accounting for only 11%.

What are acceptable fraud levels?

The answer to this question is nuanced, it's really about the cost benefit evaluation between finding a better balance between legitimate sales, cash flow and accurate fraud prevention.
In many cases fraud prevention is often poorly targeted, resulting in adverse customer service and cash flow implications.

Sadly it's often the case that merchants are not leveraging the latest technology to address their fraud exposure.

In addition to which not having a handle on fraud levels can affect revenue and the company's reputation if legitimate customer sales are affected by excessive fraud vetting measures, in addition to which bank fees or fines may be applied if fraud goes over an "acceptable" level. It would be fair to say that many merchants are unaware of the level they need to stay below to avoid these penalties.

While fraud risks are prevalent there is no reason to despair as a wide range of fraud prevention measures are available to merchants. Online retailers can achieve the levels of fraud detection required by card schemes without turning away genuine customer transactions and thereby losing income from these sales.

Shoppers and consumers are connecting with companies and retailers via various channels, using an ever-expanding choice of payment methods and devices.

This in turn creates challenges for retailers, including heightened exposure to risk and increased complexity for fraud management across a dizzying array of customer contact points.

Real-time fraud rules and neural models are used for the protection of card-not-present (CNP) transactions by less than half of the respondents. This is a particular concern given the rapid growth of CNP transactions and the corresponding growth in CNP fraud.

The introduction of EMV (EMV is a global standard for credit and debit payment cards based on chip card technology taking its name from the card schemes Europay, MasterCard, and Visa (the original card schemes that developed it) in the United States is widely expected to drive more fraudsters online.

A study last year that examined retail fraud management in this area found:

- More than **90%** of survey respondents offer multiple service and purchasing channels to their customers;
- About **65%** of them acknowledge they do not have adequate fraud management tools to support effective fraud management today;
- And only **46%** have consolidated fraud management solutions across channels to date, although most plan to do so in the near future.

How to reduce your company's fraud exposure

If Payment Card Industry Data Security Standard (PCI DSS) compliance is part of your company's operations, the PCI security standards highlight that if credit card data is exposed, it puts your customers and your brand at serious risk.

EMV chip technology combined with PCI Security Standard compliance offer a powerful combination for increasing card data security while reducing fraud exposure.

A number of approaches can be used to reduce your company's overall exposure, such as:

- Achieving & maintaining PCI DSS Compliance as a business as usual activity
- Eliminating any sensitive financial data such as customer bank account or credit card data that is no longer required. By reducing storage of such data you reduce your company's potential financial exposure should a data breach occur.
- Leveraging the latest technologies to enable staff to process customer payments efficiently, without the need to hear, see or store sensitive customer data such as credit cards & bank account data.
- Deploy real time card not present fraud analysis tools to prevent fraud before payments are approved
- Replacing in-house credit card and bank account storage with secure cloud based tokenization services will further reduce exposure to fraud and internal employee fraud.

Hackers are not amateurs; cybercrime has reached the realm of the professional and they know persistence is worth their while.

As reported by the 2013 Europol Serious and Organized Threat Assessment the

Total Global Impact of Cyber Crime has risen to *US $3 Trillion*, making it more profitable than the global trade in marijuana, cocaine and heroin combined.

Its anticipated that cybercrime will soar in the decade ahead.

This means that credit card merchants must fight cyber risks and fraud with up-to-date services and use sophisticated tools and techniques to analyze cross-merchant fraud trends and behaviors, draw informed conclusions and incorporate fraud detection tools that advance risk strategies and detect subsequent attempts in real time.

IP Solutions' ability to offer multidisciplinary card fraud detection services via advanced overlay services and call centre credit card filtering those risks can be minimised.

A fraud screening model instantly approves or rejects an order by relying on a real-time, multidimensional fraud decisioning engine. This model does not hold up orders in a review state, and so minimizes merchant resources and customer aggravation.

An effective fraud prevention strategy is vital for both online and mobile commerce — and this requires regular evaluation and assessment.

Fraud losses due to the utilization of an inappropriate fraud solution can be damaging to your business. Through careful analysis and constant communication, merchants and fraud solution providers can offer a successful multidisciplinary card fraud detection services that will help minimise fraud and boost revenue.

With the guidance of a professional, merchants should be able to track Key Performance Indicators (KPIs), which help to gauge organizational success and determine the progress of a specific approach or strategy.

When to apply online fraud screening?

When deciding how best to process payment transactions, it's important to make the decision that is right for the business, based on all available information — whether this relates to costs or benefits that can be accurately measured or other business key performance indicators that cannot be so precisely defined and assessed.

A critical point merchants have to face when determining their fraud screening measures is when to introduce fraud screening during the transaction process.

Obviously, the decision to apply screening before or after bank authorisation will have implications for business processes, transaction fees and customer experience.

Any move to adopt a different transaction flow process must be weighed carefully as it could have significant implications both financially and in terms of customer service impacts.

In addition to the calculation of actual fraud losses, analysis must take into account all fees along the payment chain, ensuring the return on investment stays positive.

Effective fraud prevention tools:

- ✓ Improve customer service.
- ✓ Increase cash flow.
- ✓ Reduce operating costs.
- ✓ Reduce fraud exposure risk.

ipsi

Fraud and mobile devices

Everyone loves the convenience of using mobile devices to make payments and to shop online, mobile banking, mobile POS facilities, m-commerce websites and mobile payment apps. All these are now an integral part of the payment landscape. Given the proliferation of mobile based customer interactions, mobile device based fraud has become a key concern for merchants and banks.

According to recent research, about 48 per cent of all fraudulent transactions were attributed to the mobile channel in Australia. The report determined that merchants are paying more per dollar of mobile fraud.

The overall mobile channel cost grew from $2.83 in 2013 to $3.34 in 2014.
Hackers are well aware that mobile payments, whether through a physical POS terminal or online, are open to risk as smartphone deployments may not meet security best practice: technical security measures are less common, operating systems are updated less frequently and mobile social networking applications sometimes lack detailed privacy controls.

In addition, mobile malware has experienced a 400 per cent increase in recent years and mobile shoppers using web browsers can be more vulnerable to attacks such as phishing and website spoofing.

About 48 per cent of all fraudulent transactions were attributed to the mobile channel in Australia.

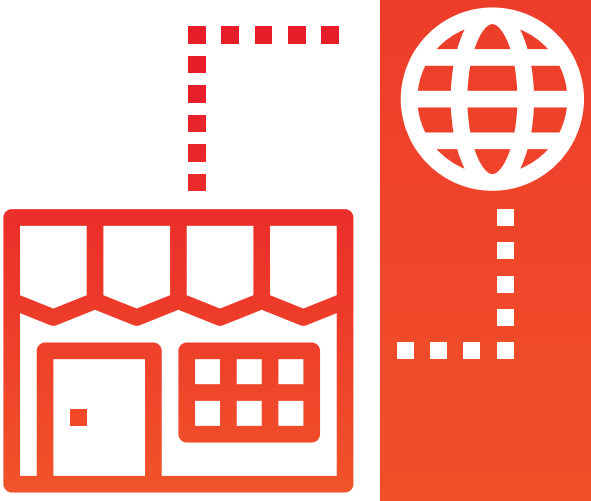
Fraud screening processes

The merchant must decide whether they prefer to manage confirmed or attempted sales. If, for example, the merchant operates a no-challenge policy — working on astraight accept/deny recommendation — there would be logic in handling fraud screening post-bank authorisation, when the precise value of the sales being denied is clear.

Essentially, there is no incorrect choice.

On the other hand, a merchant operating in an industry with higher levels of attempted fraud and higher transaction values might seek the more accurate fraud detection provided by better key performance indicators in the pre-authorization scenario. It's a decision that needs thought and planning.

When considering whether to screen pre-or-post-authorisation, a merchant will need to assess the operational impact of a new transaction flow, potential cost savings and the implications for customer relationships.



ipsi

If you represent a medium to large business and you wish to prevent your business from becoming the next cybercrime or card-not-present fraud statistic,

Please speak to a member of our ecommerce or PCI DSS team about safe guarding your business today.

Click here to BOOK NOW

ipsi

1300 975 630
www.ipsi.com.au

Jones Bay Wharf
6, 26-32 Pirrama Rd,
Pyrmont, Sydney NSW 2009 Australia