REPORT

McAfee
Together is power.

The Hidden Data Economy

The marketplace for stolen digital information

Table of Contents

Authors

This report was researched and written by:

- Charles McFarland
- François Paget
- Raj Samani

Introduction

Data is the "oil" of the digital economy. The commercial market for personal data is booming, with large databases of subscriber information driving up the enormous valuations of those companies that own it, even though many have yet to turn a profit. As the commercial value of personal data grows, cybercriminals have long since built an economy selling stolen data to anybody with a computer browser and the means to pay.

In the 2013 McAfee® Labs report ***Cybercrime Exposed: Cybercrime-as-a-Service***, we demonstrated how current tools, products, and services can allow anyone to become a cybercriminal, regardless of technical ability. We followed up with the report ***Digital Laundry: An analysis of online currencies***, and their use in cybercrime, which explained virtual currencies in detail and how they are used to convert stolen data into cash. By the time Digital Laundry was published in 2013, the publicity following **the law enforcement action against the Silk Road** let the world know that illegal products could easily be acquired online. Such actions have demonstrated just how much traditional crime has evolved with the help of the cyber world.

Cybercrime Exposed and *Digital Laundry* focused on tools that aid an attack. This report will attempt to answer the question: What happens after a successful breach?

Immediately after the Target breach, I cowrote a blog that tracked the sale of stolen credit cards and showed that much like traditional economics, the price of stolen credit cards went down with the huge influx of new stolen cards on the market. The Target example is only the tip of the iceberg. This paper provides more detail on this hidden data economy.

—Raj Samani, CTO of McAfee for Europe, the Middle East, and Africa

Twitter@Raj_Samani
Twitter@McAfee_Lab@McAfee_Lab

We will highlight why apathy among victims of a data breach, and ultimately those data subjects whose information is being sold, may be costly.

Connect With Us

Hidden in Plain Sight

The title of this report suggests that there exists a hidden doorway into an underground marketplace for nefarious products that is not accessible to us muggles. In reality, this marketplace is not nearly as well hidden as we imagine, and it certainly does not require prior knowledge of a secret public house and its hidden courtyard. ***Cybercrime Exposed: Cybercrime-as-a-Service*** highlights just how accessible these products, tools, and services are to anybody with a browser. Although we do not intend to repeat the findings from that earlier report, the world has moved on since it was written two years ago.

What has changed? This underground marketplace has evolved to include almost every conceivable cybercrime product for sale or rent. We correctly predicted that the rise of this "as-a-service" model would act as a key driver in the growth of cybercrime. The recently published ***McAfee Labs Threats Report: May 2015*** provides evidence of this with the rise of the ransomware CTB-Locker. The authors of CTB-Locker established an affiliate program as part of their business strategy: Affiliates use their botnets to send spam to potential victims; for every successful infection in which the victim pays the ransom, the affiliate gets a percentage of the money.

The growth of the as-a-service economy across all components of an attack (research, cybercrime tools, and infrastructure) continues to grow, and none more so than hacking-as-a-service, in particular on how stolen data is made available. We will highlight why apathy among victims of a data breach, and ultimately those data subjects whose information is being sold, may be costly.

A sad side effect of reading about data breaches is the concept of "data breach fatigue," which is another way of saying "apathy." The recent article ***I Feel Nothing: The Home Depot Hack and Data Breach Fatigue*** provides a wonderful example of such apathy:

> "Because banks are responsible for making us whole if our credit cards are misused, and we are simply issued new cards (an annoying hassle, but not life altering), I join you in reacting to news of these hacks with a shrug," the author writes.

Although disillusionment may be understandable given the steady stream of breach notifications and stories detailing the theft of millions of records, it is important to recognize that this is data about us. Our information is being openly sold, and the individual repercussions may not be felt for some time.

This is why we are publishing this report: to combat the sense of apathy. We do not intend to spread fear, but we want to explain why we as a society should be concerned when we receive notifications of breaches as we consider proactive measures to reduce the likelihood of becoming victims.

A final comment: We don't know if the many examples in this report are authentic or are tied in any way to the brands, as the sellers claim. Indeed, the excellent reputation of such well-known brands is frequently used by thieves as the basis to promote this sort of online fraud.

Financial Data

Selling stolen financial data is a relatively broad topic, with a multitude of data types for sale and marketplaces that vary between the visible web via a standard browser and the "dark web" through other access methods.

Data breaches involving the theft of financial data, particularly payment card information, continue to dominate headlines. Particularly impacting retailers, the theft of such information invariably results in this data appearing on the visible web. Payment card information made available in those marketplaces will vary in price based on a multitude of options. A snapshot of these options is shown in the following table.

The preceding categories relate to the information available along with the payment card number:

- "CVV" is the industry acronym for card verification value. CVV1 is a unique three-digit value encoded on the magnetic stripe of the card. CVV2 is the three-digit value printed on the back of the card.
- "Software-generated" is a valid combination of a primary account number (PAN), an expiration date, and a CVV2 number that has been generated by software. Valid credit card number generators can be purchased or found for free online. As these tools can be easily found, their generated combinations do not have market value.
- "Random" refers to a card number chosen randomly in a hacked database. It is random for the bank and card type.
- "Fullzinfo" means the seller supplies all of the details about the card and its owner, such as full name, billing address, payment card number, expiration date, PIN number, social security number, mother's maiden name, date of birth, and CVV2.

Occasionally, additional information is available for sale. Payment card data that includes "with COB" refers to those cards with associated login and password information. Using these credentials, the buyer can change the shipping or billing address or add a new address.

Some sellers will not provide the data after purchase. After all, whom will the buyer complain to in the event that the stolen information is not delivered? However, as depicted in the following image, many sellers will deliver stolen card information with all associated information.

Payment Card Number With CVV2	United States	United Kingdom	Canada	Australia	European Union
Random	$5–$8	$20–$25	$20–$25	$21–$25	$25–$30
With Bank ID Number	$15	$25	$25	$25	$30
With Date of Birth	$15	$30	$30	$30	$35
With Fullzinfo	$30	$35	$40	$40	$45

Table 1. Estimated per card prices, in US$, for stolen payment card data (Visa, MasterCard, Amex, Discover). Source: McAfee Labs.

Figure 1. Payment card data with additional information.

Buyers have many options, including the geographic source of the card and the card's available balance. Both of these options impact the price of a card, as we see in the following table.

Dump Track With High Balance	Price
Track 1&2: PinATM United States	$110
Track 1&2: PinATM United Kingdom	$160
Track 1&2: PinATM Canada	$180
Track 1&2: PinATM Australia	$170
Track 1&2: PinATM European Union	$190

Table 2. Dump track prices per card. Source McAfee Labs

The term *dump* refers to information electronically copied from the magnetic stripe on the back of credit and debit cards. There are two tracks of data (Track 1 and Track 2) on each card's magnetic stripe. Track 1 is alphanumeric and contains the customer's name and account number. Track 2 is numeric and contains the account number, expiration date, the CVV1 code, and discretionary institution data.

List prices are variable, based on supply, balance, and validity. Some of these factors are detailed in the following image.

Figure 2. Payment card shopping lists.

As the preceding image illustrates, buyers have many choices.

The sale of payment card data is common, and is well documented **in a recent series of McAfee blogs**. However, such payment cards are not the usual type of financial data targeted and subsequently sold on the open market. Much like cards, online payment service accounts are also sold on the open market, with their prices determined by additional factors. Such factors are, however, considerably more limited than those of payment cards, with the balance the only defining factor influencing prices, as we see in the following table.

Online Payment Service Account Balance	Estimated Price per Account
$400– $1,000	$20– $50
$1,000– $2,500	$50– $120
$2,500– $5,000	$120– $200
$5,000– $8,000	$200– $300

Table 3. Online payment service accounts for sale. Source McAfee Labs

The prices in this table are estimates. We have seen many examples of services for sale that fall outside of these price ranges.

Everything is available. In the following images, we see bank-to-bank transfers offered for sale, and the availability of banking login credentials.

Figure 3. Example of bank login credentials for sale.

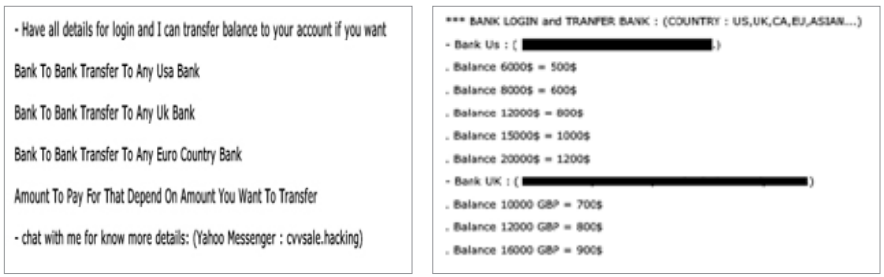

Figure 4. Example of bank login data for sale.

There will always be suspicions about the validity of the products for sale, as many individuals have paid for stolen financial data only to not receive what they expected. One seller refers to this dishonor among thieves within their opening pitch:

> "ARE YOU FED UP OF BEING SCAMMED, AND RIPPED? ARE YOU TIRED OF SCAMMERS WASTING YOUR TIME, ONLY TO STEAL YOUR HARD-EARNED MONEY?"

This particular seller, though not offering free credit cards that a buyer could use as a test, does offer a replacement policy for any cards that do not provide the advertised balance. Other methods of ensuring a seller's honesty include the use of social validation, with positive feedback from other buyers. Forums are full of helpful advice from buyers who have successfully negotiated purchases as well as which sellers to avoid.

> "Hey man, don't know if you know this, but [redacted] pulled a exit scam on evo?
> as far as i know, he pulled an exit scam, then he came back saying his friends had screwed him over, asked people to pay like 4BTC to join his official priviate reselling club. he then just disspeared again.
> in fact theres a guy called Underwebfullz (or somthing like that) whos doing the same thing on alpahbay, so people think its him"

Sellers who employ sophisticated sales and marketing efforts are leveraging YouTube to advertise their wares to potential customers. The videos often attempt to provide some degree of visual confirmation for prospective buyers that they can be trusted, although such approaches can backfire through comments associated with the videos.

Login Access

Other types of data for sale include access to systems within organizations' trusted networks. The types of entry vary, from very simple direct access (such as login credentials) to those that require a degree of technical competence to carry out (such as vulnerabilities).
In the following image we can see the availability of vulnerabilities that allow potential buyers access to bank and airline systems located in Europe, Asia, and the United States.

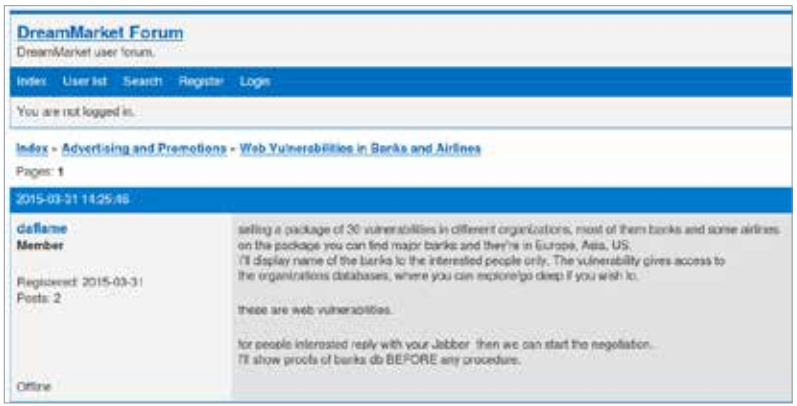

Figure 5. Example of access to bank and airline systems for sale.

As with the sale of financial data, sellers strive to offer a degree of proof to prospective buyers that their offers are valid.

Recent research by cybercrime expert Idan Aharoni suggests that the types of systems criminals sell access to now include critical infrastructure systems. In his article **"SCADA Systems Offered for Sale in the Underground Economy,"** Aharoni included one example in which a seller provided a screenshot that appears to be a French hydroelectric generator as evidence that the seller had access.

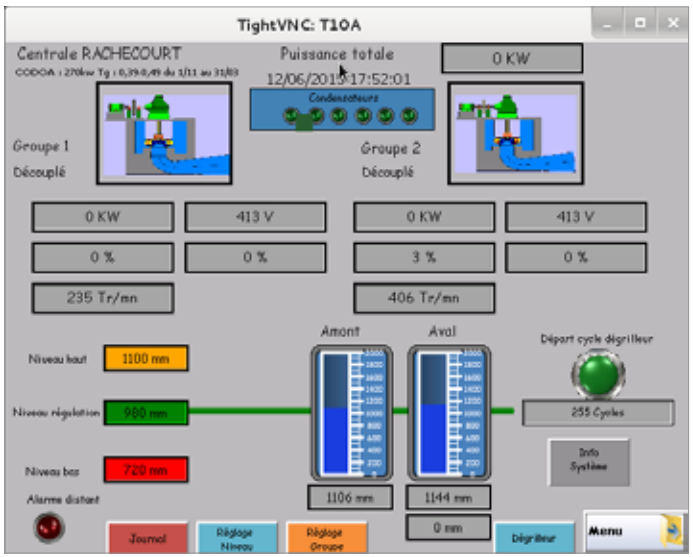

Figure 6. One seller claims that this is a screenshot of a French hydroelectric generator, used as evidence that the seller has access to a critical infrastructure SCADA system.

As with previous examples, a buyer can question whether the access offered is indeed valid. It would not be particularly difficult to produce a screenshot and imply this represents access; yet this message does represent a very worrying trend (as Aharoni points out).

Stolen enterprise data is also for sale. In the following figure we see a seller offering data stolen from a university.

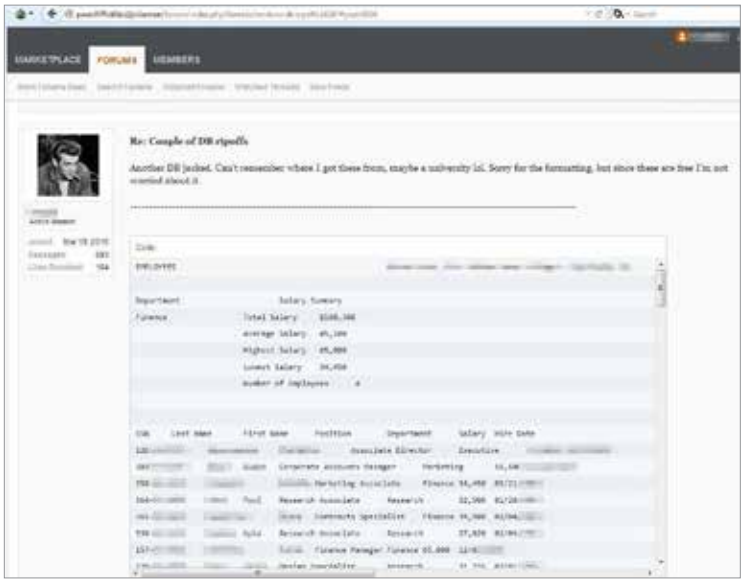

Figure 7. Example of stolen information from a university offered for sale.

Access to Online Services

Many people subscribe to digital services, including music, videos, loyalty programs, and others. Because such accounts are relatively inexpensive, one might assume that information from them would not offer a sufficient return. Despite such economics, however, the availability of such accounts is widespread across multiple marketplaces, which suggests a demand among prospective customers.

When a stolen online account becomes compromised, the legitimate owner can be impacted in a variety of ways. The account can be held or closed due to malicious activity by the buyer—sometimes causing weeks of support calls. A victim could also suffer financial losses from the purchase of items with stored credit card information, or lose access to free perks such as loyalty points collected during the lifetime of the account. Worse, there are circumstances in which the impact is quite disturbing.

The following image shows one example of online service accounts for sale.

Figure 8. Example of online video streaming accounts for sale.

Are online video streaming users the only victims? Hardly. The sad reality is that access to just about every conceivable online service is available. We found another online video streaming service account selling for $0.55. With single accounts to digital services selling for less than a dollar, criminals must move a lot of online accounts to make their efforts worthwhile.

Figure 9. Other online video streaming service accounts are for sale for less than $1.

Many online streaming entertainment media services are commonly sold. Both HBO NOW and HBO GO accounts can be found for less than $10 as well as other cable TV-branded streaming services. Clearly, video streaming services are in high demand. Even premium professional sports streaming services can be purchased for $15. We also found other online accounts being sold, including lifetime subscriptions to premium pornography accounts, as well as free referral links to the dark web market Agora.

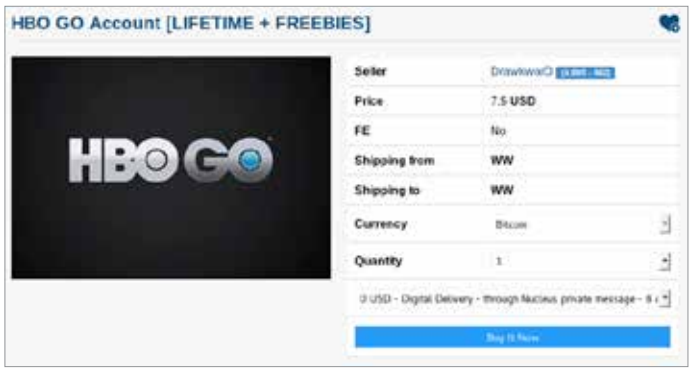

Figure 10. Example of access to an HBO GO account for sale.

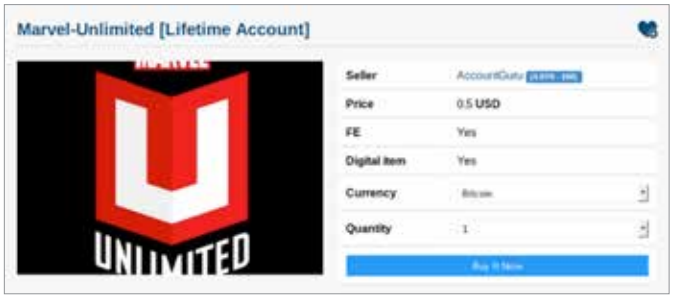

Figure 11. Cyberthieves sell Marvel Unlimited accounts for cheap access to digital comics.

Even free online accounts attract criminals. The following image shows a hotel loyalty account with 100,000 points on sale for $20. Customers legitimately open these accounts at no cost, and yet there is a market for them, resulting in the loss of accumulated perks that sometimes take years to accrue.

Figure 12. Even hotel loyalty programs are for sale.

One motivation for purchasing stolen online account access is to hide the buyer's reputation, either due to bad business practices or outright fraud. A buyer wishing to acquire a new online auction community business identity can pay plenty, but an established account with good history can be valuable.

Figure 13. An online auction account for sale.

For less stringent needs, online auction accounts are available in packs of 100 for a range of account types.

Figure 14. A credit card sales location that also offers access to online auction accounts.

Identities

The sale of a victim's identity is the most frightening category because it is so personal.

McAfee **recently collaborated** with law enforcement in Europe to take down the Beebone botnet. This botnet was able to download malware—including ZBot banking password stealers, Necurs and ZeroAccess rootkits, Cutwail spambots, fake antivirus, and ransomware—onto the systems of unsuspecting users. We are dismayed at the lack of remedial action taken by users, and in particular those based outside of the United States and Europe. **Raj Samani's blog on this topic** said that a vast section of society fails to appropriately protect their data—often with significant ramifications.

In the following image we have an example of a person's digital identity stolen by cyber thieves. A prospective buyer could take control of this individual's digital life—social media, email, and more. (We have shared this information with law enforcement in the United Kingdom.)

Figure 15. Example of an identity for sale.

The preceding example, though rich in information, requires the buyer to wade through lots of text. But some sellers offer a more graphical interface to appeal to prospective buyers. The following example lets buyers choose individuals by their email accounts, the first step to taking control of other parts of the victims' lives.

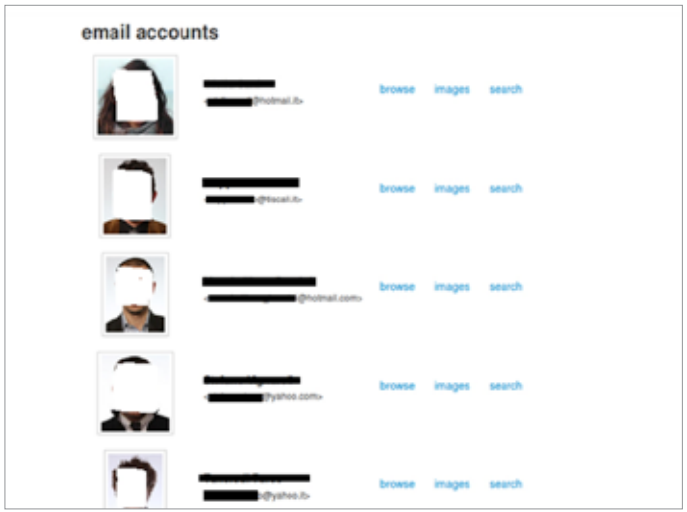

Figure 16. This service lets buyers easily choose a profile.

Closely related to the marketplace for stolen identities is the marketplace for stolen medical information. Such data is not as easy to buy as payment card data, but sellers of medical information are online. Security journalist Brian Krebs discussed this in his article "**A Day in the Life of a Stolen Healthcare Record**," in which a "fraudster leaked a large text file [that] contained the name, address, social security number, and other sensitive information on dozens of physicians across the country." (See following image.)

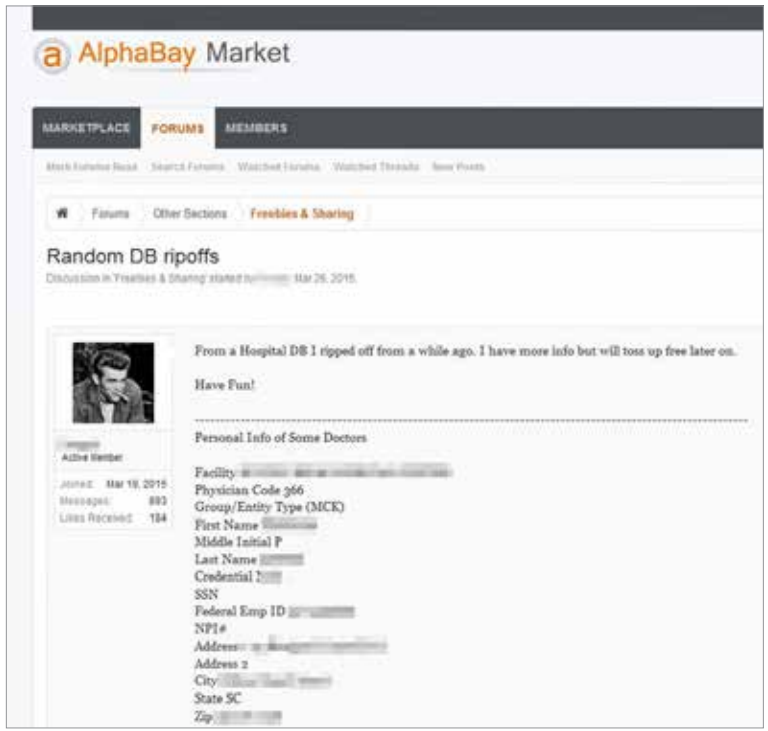

Figure 17. An example of information stolen from a medical service offered for sale.
Source: Krebs on Security.

Although the majority of this report highlights the sale of stolen data, stolen data is sometimes openly shared without cost. In the following image, the hacker collective Rex Mundi **disclosed identifiable patient data** because the Labio service did not pay them a ransom of €20,000.

Figure 18. Hackers revealed private customer information to punish a medical company for not paying a ransom.

Conclusion

The examples of the hidden data economy in this report represent only the tip of an iceberg. We omitted many other categories and services, but we hope these examples make the threat clear. In this report we discussed stolen data offered for sale. Cybercriminals also buy products that enable attacks. This includes the purchase and rental of exploits and exploit kits that are fueling an enormous number of infections across the world. Cataloging the available offers is impossible because the field is growing at a tremendous rate.

When we read about data breaches, the cybercrime industry may seem so far removed from everyday life that it is tempting to ignore the message. However, cybercrime is merely an evolution of traditional crime. We must conquer our apathy and pay attention to advice for fighting malware and other threats. Otherwise information from our digital lives may appear for resale to anyone with an Internet connection.

About McAfee Labs

McAfee Labs is one of the world's leading sources for threat research, threat intelligence, and cybersecurity thought leadership. With data from millions of sensors across key threats vectors—file, web, message, and network—McAfee Labs delivers real-time threat intelligence, critical analysis, and expert thinking to improve protection and reduce risks.

www.mcafee.com/us/mcafee-labs.aspx

About McAfee

McAfee is one of the world's leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions that make the world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com.

McAfee™
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com