

Revolutionizing QSR Multi-Unit Operations and Loss Prevention

How Dunkin' Brands Will Save Hundreds of Millions of Dollars in Revenues by Controlling Internal and External Fraud

By James McDonald,
Physical Security Consultant

*"Your employees will only do what you expect,
if they know that you're going to inspect."*



© 2009 by James McDonald

Copyright holder is licensing this under the Creative Commons License, Attribution 3.0
<http://creativecommons.org/licenses/by/3.0/us/>

**PLEASE FEEL FREE TO POST THIS ON YOUR BLOG OR
EMAIL IT TO WHOMEVER YOU BELIEVE WOULD
BENEFIT FROM READING IT. THANK YOU.**

Table of Contents

Introduction	5
How Do Most Restaurant Employees Steal?	8
Cash Larceny	8
Skimming	8
Sweethearting	9
Introduction to Employee Theft, Fraud and Loss Prevention	9
Why People Steal or Commit Fraud	10
Opportunity	10
Rationalization	10
How Did Dunkin' Employees Steal.....	11
How I Learned about the Dunkin' Brands Opportunity	12
Who Was Really My Customer?	14
• Dunkin' Brands, Inc. ("The Brand")	14
• Brand Advisory Council – (BAC).....	15
• The National DCP, LLC (NDCP).....	16
As you can see, I had my hands full both Politically and Technologically	16
Why Did I Believed That March Networks Offered the Best Solution?	17

The Lab Tests.....	18
The Trials and the IT Sub-Committee	19
In Conclusion	20
Contact Information	21

Introduction

Thank you for your interest in this e-book. In it I describe my sales experiences and how I perceived the needs and opportunities of offering fully integrated video surveillance solution in the Quick Service Restaurant (QSR) industry and other retail markets. In particular I want to tell the story of my experiences developing and selling Dunkin Brands and why I believe we were so successful. “Revolutionizing QSR Multi-Unit Operations and Loss Prevention” Revolutionizing: defined for our purposes here is defined as “To bring about a radical change.” My purpose within these pages is to give you my experiences and motivations that today are proven to help any retail end-user become more profitable and efficient using a technological countermeasure solution. If you are reading this you may be an end-user looking for a new surveillance solution for your organization or you may be a video surveillance manufacturer wondering why you don’t sell very many systems to franchised chains, or you could be a great salesperson wondering how you bag the elephant and make the big sale, my wish is that you, the reader, can benefit from some of the concepts and ideas that are discussed within these pages.

As a student of physical security and loss prevention, the sources of information I have collected over the years are vast. I have read and collected many articles, studies and books on specific and related subjects concerning, security, loss prevention, operations and human behavior. I want to acknowledge two Associations which have been an active member and have lead me in the direction to learn more and where to look to find the answers to the questions I developed thru my experiences. First, *The Association of Certified Fraud Examiners* (ACFE) located in Austin, Texas and on the web at <http://www.acfe.com/home.asp> and *ASIS International* (ASIS) located in Alexandria, Virginia and on the web at <http://www.asisonline.org/>. Both of these fine organizations have local chapters around the world

and very supportive members. I personally recommend membership in both organizations for all of my colleagues, clients and prospects. I can't say enough regarding the knowledge and support that I have received from these two professional organizations. Additionally I recommend that if you are a retailer or if you market to retailers you become a member of the *National Retail Federation* located in Washington, DC and on the web at <http://www.nrf.com> this group has an excellent Loss Prevention sub-group and a great relationship with federal and local law enforcement. There are many other industry and vertical industry associations I follow and support, for a full list of the links go to my main website <http://www.PhysicalSecurityTechnologist.com> and click on the "research" tab.

I normally do not discuss any recommended solutions or countermeasures for a client. However, I recently read an article written by John (Jack) L. Sullivan, the Director of Loss Prevention and Certified Fraud Examiner at Dunkin' Brands. In this article Jack described his perspective on the custom solution that March Networks Corporation and I tweaked, tested, taught and worked on over a two year period. A copy of Jack's publication is available and can be downloaded at the March Networks website [http://www.marchnetworks.com/Files/Reprint Dunkin Apr09.pdf](http://www.marchnetworks.com/Files/Reprint_Dunkin_Apr09.pdf). Since I was the main catalyst that brought these two organizations together initially, I felt inspired to add my comments. I have always defined my role in my current profession as helping end-users by designing solutions that combined three main elements:

- Physical Security Technology (***protecting physical assets***)
- Loss Prevention & Occupational Fraud Prevention Tools (***protecting of financial assets***)
- Risk Management Policies and Procedures (***protecting from potential legal liabilities***).

My goal of any final solution or recommendation is that it can be easily and regularly monitored by management personnel. My goal has never been to only catch employees stealing, even though we do.

My goal has always been to create an environment that eliminates all negative behaviors that can affect stores profitability.

In 1978, I became a restaurant manager. At that time and even today I have believed in the concept of “Trust, but Verify” meaning *your employees will only do what you expect, if they know that you're going to inspect*. I learned to inspect all employees work constantly. I learned if you wanted to be the best restaurant, you needed to demand and enforce high expectations from your employees every day. I would verify their appearance, customer service, and their “side work” before they finished their shifts. Today’s technology allows management to remotely verify all types of activities and behaviors, so that employees will perform their tasks correctly, knowing that if they don’t they will be held accountable.

Now let me discuss my perspective on the Dunkin Brands (The Brand) Video Surveillance Solution and how I worked together with key manufacturers and “The Brand” to eliminate opportunity and temptation from the workplace and create a win/win/win solution for everyone.

I believe that most employees will not steal if they believe that they will be caught. According to research conducted by the Association of Certified Fraud Examiners (ACFE), U.S. organizations lose an estimated 7 percent of annual revenues to fraud. Based on the projected U.S. Gross Domestic Product for 2008, this percentage indicates a staggering estimate of losses, to occupational fraud and abuse (their definition), to be around \$994 billion among all organizations. Despite increased focus on anti-fraud controls in the wake of Sarbanes-Oxley and mandated consideration of fraud in financial statement audits due to SAS 99, their data shows that occupational frauds are much more likely to be detected by a tip than by audits, controls or any other means. Forty-six percent of the cases in this Report were detected by tips from other employees, customers, vendors, and other sources. Tips were also the most common means of detection in 2002, 2004, and 2006. The ACFE's [2008 Report to the Nation on Occupational Fraud & Abuse](#) details the survey results of 959 Certified Fraud Examiners (CFEs)

throughout the US. I have found those businesses that are primarily cash such as: restaurants and bars have a higher loss rate than the 7% average. In Jack's article, some of Dunkin' Donuts locations have seen an immediate increase of up to 30% in sales over similar stores in the same DMA (Designated Market Area) that were not yet using the system.

How Do Most Restaurant Employees Steal?

As a manager I quickly learned the concepts of *sweet-hearting*, *cash larceny* and *skimming*, or how my employees will steal from me. At the time we had manual cash registers, nothing like the point-of-sale systems of today. It was easy for an employee to give away food, they would take money and look like they were making change; in reality they might take a five dollar bill and give the friend back four one dollar bills and 4 quarters on a \$1.50 charge. If they gave back extra change the drawer would be short, but with 6-10 employees working out of the same drawer it would be hard to find the thief. Most managers blamed this on poor training, or over portioning. Employee theft was not thought to be the major culprit. No one wants' to think their employees are stealing from them. What are the three biggest areas of occupational fraud and theft? They are *Cash Larceny*, *Skimming* and *Sweethearting*.

Cash Larceny

Simply defined is any scheme in which cash receipts are stolen from an organization after they have been recorded on the organization's books and records.

Skimming

Skimming for the purposes of our discussion here is the removal of cash from an organization before the cash has been recorded in the organization's books. Because the money is stolen before it appears on the books, skimming is known as "off-book" fraud. Basically the employee pockets the cash directly from the customer.

Sweethearting

In retail, "sweethearting" is one kind of theft carried out by collusion between an employee and a customer. It is so named because it most often occurs between a cashier and his or her family members or friends, usually with prearrangement.

I was always very successful in detecting a thief(s) for some reason, so after a short time the district, regional and divisional managers quickly figured out that they could use me to help with loss prevention issues in other store locations. If the numbers were off in a store and the normal audit(s) did not show why, I would be transferred into the store to verify if all company policies and procedures were being followed. I could quickly figure out if food was disappearing out the back door. In other words, if the loss was a food cost issue or if the managers were stealing cash from the registers. We caught employees stealing cases of food, especially steaks and chicken. I also caught managers skimming thousands of dollars from the registers. The techniques I used then were very simple, but the concepts themselves are the same as I use today. Today I just use the technology to see remotely, what I would watch for in person twenty five years ago. In the twelve years working in restaurants, the skills I developed in loss prevention have always stayed with me. Both understanding the scams used by employees to perpetrate a fraud and the reasons why they would take the risk in the first place. This knowledge would stay with me throughout my career.

Introduction to Employee Theft, Fraud and Loss Prevention

In early 2001 when I started to sell digital video recorders (DVRs) for a company out of New York I again became a student of loss prevention and began to research employee theft and fraud. I would read everything I could get my hands on and develop documents that I could use as sales tools to help small business owners understand the risks that they were facing. At the same time I developed policies and procedures that I would give to my customers to help them get immediate results.

Why People Steal or Commit Fraud

The best way I found to explain why people commit negative behaviors such as theft and fraud is illustrated by the Fraud Triangle. My source of this idea was the late Donald R. Cressey (1919-1987) he was a central figure in twentieth century American criminology. A distinctive feature of criminology since the 1930s has been the dominance of sociology among the various disciplines studying crime and criminal justice. There are categorically three reasons why someone typically commits occupational fraud and abuse - and these reasons make up the fraud triangle (shown here). Think of it as a three legged stool, if you take a leg away, it will fall over.



Financial Pressure usually comes from two places; inside the employee's company in the form of job pressure or the pressure to meet deadlines and revenue goals, and external pressures such as family life, financial troubles, illegal drugs, extra marital affairs, the recession, etc.

Opportunity is the way that the employees believe that they can get away with it - and therefore it is primarily this part of the fraud triangle that I work with to eliminate temptation by enforcing certain types of controls such as video surveillance.

Rationalization almost doesn't have to be explained - most of us are very good at it. But most of the time the argument is "My company doesn't recognize my efforts." "They owe it

to me. I deserve to get paid more," or "I'm only borrowing the money. I'll pay it back," or "Nobody will miss it." "The company can afford it," or "Everyone does it. I'm not hurting anyone."

In my experience most of these acts start out small and grow over time. I had one manager who told me he started with \$20 by accident. He made brought change to the register and when he got home the twenty dollar bill was still in his pocket. No one noticed so \$20 became \$100, then \$200 and so on. What happens is that within a short period of time the money they are stealing is no longer discretionary income, it becomes part of their weekly budget. I found this to be true especially in bartenders. Whenever I installed a system in a bar I would tell the owner that he will probably lose some of their staff. I would say “They will have to get a job somewhere else, where they can continue to steal.”

All three elements need to exist in order for the occupational fraud or theft to occur. – I could never do anything about financial pressure and as far as rationalization goes, that was up to the business owner. However, as a security professional I could attack “Opportunity & Temptation” if I could get the employees to think that they would be caught if they tried to steal, then I would break the cycle. I would look to physical security technologies to see how they could be used as a key fraud or theft countermeasure.

How Did Dunkin’ Employees Steal

Whenever I work with a new company I do research, I find out as much information as I can, when I looked into Dunkin’ I found many websites with comments on how to steal from the company as an employee. When I was preparing for this writing I searched again, guess what I found? If you Google “How to steal from Dunkin’ Donuts” and you will find this page that describes many negative behaviors go to <http://everything2.com/title/Working%2520at%2520Dunkin%2527%2520Donuts> the following is what I call it the “**Dunkin’ Employee Fraud Manual**”, I hope you find it as interesting as I did, here is a sample of the page.

“The training videos will emphasize “up selling” as a major part of your job, but don't be fooled! Dunkin' Donuts is different from any other fast food restaurant because there is a tip cup. When working at Dunkin' Donuts, your major concern should be how to increase the money in your tip cup without getting fired, that's it! Forget about being a model employee, nobody gives a rat's ass. Your efforts, however big or little, do not matter if nobody is watching, so throw your morals and ethics out the window. You are now an underpaid worker in a shit job, so think accordingly.”

After reviewing this website and others like it I was confident that the return-on-investment for Dunkin would be above average. It also gave me a game plan to review potential behaviors within their POS systems if I made it to the system's “trial or test” phase. In the following pages I will outline the process and more importantly my perception and point of view within the process that I believe was the reason(s) the March Networks solution was chosen.

How I Learned about the Dunkin' Brands Opportunity

I early February, 2006 I was working with a Boston based Point-Of-Sale (POS) Company who was developing a proprietary XML interface from their POS system to a digital video recorder or DVR. They had asked me to help them complete the development and testing of the software and to cross train their sales people to sell DVRs to their existing client base and to new prospects. I had just left working for a west coast manufacturer of DVRs which was built on a Windows Personal Computer (PC) platform. I had previously worked for another Windows DVR manufacturer on the east coast and I was looking to get away from those types of platforms because of all of the customer service issues. I felt that 80% of my customer's service issues had nothing to do with the software or the hardware but were related to the Windows Operating System which allowed the customers employees to use the devices to check the internet and their email allowing viruses and other issues to infect the systems.

My new employer had found a Canadian company called March Networks whose operating system was their own Linux based system, eliminating all of the Windows issues that I had become accustomed. I wanted to create a leasing program for this new system, so I contacted a company I had worked with in New Hampshire when I was selling DVRs to Subway and McDonald franchisee's the year before.

At our initial meeting their manager Peter Tupper told me, by the way, Dunkin' Brands had just released a Request-for-Information (RFI) to find a new video surveillance solution. Peter's company was already involved in financing Dunkin' Brands franchisees. When I got back to my office I started my quest to reach out to the company to get a copy of the RFI. At the same time Dunkin' Corporate was going thru some management changes. Dunkin' Brands, Inc. was being purchased by Bain Capital LLC, The Carlyle Group, and Thomas H. Lee Partners, L.P. I had reached an IT manager on the phone, discussed my ideas and set up an appointment a few days later.

At the same time I had a meeting set up with Mr. David Uberig, a dealer representative with March Networks to review the March System and get me up to speed on their devices and software and to review with him what we were doing with regards to our POS interface. While David was in town, together we took a ride to Dunkin's Corporate Headquarters, meet with the IT manager. He was unable to meet with us at that time, but we were able to meet briefly with one of his colleagues and she promised us that we would get a call from the person in charge of the RFI. He did call me a few hours later, we received the RFI and scheduled an appointment a few weeks later to present our original presentation that discussed the basic capabilities of the March Networks Systems and answered all of the questions in the RFI. Over 40 vendors responded to the RFI but only 12 were asked to present their solutions in person to the IT department.

Who Was Really My Customer?

It is important here to understand that I had multiple customers to understand within the Dunkin' Brand's universe. We had Dunkin' Brands, Inc., Corporate called "The Brand," the Dunkin' Franchisee's, Brand Advisory Council – (BAC) represented here by their IT Sub-Committee and The National DCP, LLC (NDCP) is the exclusive Supply Chain Partner for Dunkin' Brands, Inc. My real customer was the Franchisees because they actually purchased the system. I had sold other systems in the past to Dunkin' Franchisees directly as well as to other groups. Most franchisors had no real control and let their franchisees do whatever they wanted, that all was about to change.

It always comes down to money; let us break down how I saw the needs and concerns and motivation of each group.

- ***Dunkin' Brands, Inc. ("The Brand")***

The overall focus of The Brand was to protect the brand, grow the brand and collect their franchise and royalty fees. The Brand had two departments that were very interested in the video surveillance project. They were the IT Department and the Loss Prevention Department.

- The **IT Department** who headed up the initial research of the marketplace and issued the RFI and was trying to find the best solution that would fill everyone's needs and protect their network at the same time. A main issue at the time, in 2005-2006, was created by a group of major credit card companies; the Payment Card Industry Data Security Standard (PCI-DSS) <http://www.pcistandard.com/home.html> comprised a set of security guidelines that are designed to help retailers prevent credit card fraud and identity theft. In a nutshell, any company that processes, stores, or transmits credit card numbers must comply with the PCI DSS standard. Visa International, MasterCard, Worldwide, Discover Financial Services, JSI, and American Express all require PCI compliance of the retail companies that run their

customers' credit cards. And any company that fails to comply with the requirements may risk stiff penalties. I believed that the March Networks solution could best deal with these concerns.

- The **Loss Prevention Department** which was headed by John Sullivan, CFE, Director of Loss Prevention and former federal agent. I did not get to meet Jack until much later in the process but my understanding at the time was that the department was primarily looking for franchisee royalty fraud not directly attacking employee theft at the store level working with individual franchisees who were dealing with employee theft issues. At the time I had sold some five thousand DVRs primarily to QSRs and convenience stores and I believed that the real issue was a franchisee, owning multiple units, trying to attack opportunity and temptation as well as other operational issues that could be solved with an integrated video solution with remote access. I had a plan to prove my theories to LP.
- **Brand Advisory Council – (BAC)**

The IT Sub-Committee of the BAC was directly involved from the beginning. They all wanted the best solution at the best price. Another major concern of the franchisees was the network. Each franchisee was already paying for the company's virtual-private-network (VPN) and they wanted the new system to run on the network that they were already paying monthly fees. The main issue here was that the initial network was designed for very limited use, primarily just data for credit card and gift card approvals and polling of sales data, not video, so there was a natural bandwidth and infrastructure and network security issue. I did get to work with many members of this group, giving all who asked a free installation of my system design for them to use and test on their own and at no cost.

- ***The National DCP, LLC (NDCP)***

The DCP's primary focus is procuring, contracting and delivering the food, packaging and equipment needed to operate these consumer-loved concepts each day. However, they also manage the IT infrastructure that connects each store to the nationwide VPN. Established in 2005 to unify both the buying power and manpower of four existing regional centers, NDCP is a co-operative that is owned and operated by the franchisees of the Dunkin' Brands system. The DCP concerns were twofold. First they were very concerned about the potential network issues. They also had an interest in the distribution of the final product solution. Dunkin was developing a "Store-in-a-Box" concept that would ship everything needed by a franchisee to open or re-model a Dunkin' Donuts location.

As you can see, I had my hands full both Politically and Technologically. My key points of concern, from a sales point of view were:

- Prove the March Networks Operating System and Software would work for all parties.
- Prove that the March Networks Software could interface with the two main POS systems that were deployed. (We needed to build out data translators for both Sharp Cash Registers (80% of the deployed population) and Radiant Systems POS solution the new choice of the IT department.)
<http://www.radiantsystems.com/news/press-releases/2007/081507.htm> .
- Prove the Loss Prevention benefits of the March Networks to the Brand and to the Franchisees.
- Build trust and political allies within the Brand, the Franchise Organization and the DCP.
- Solve all deployment, infrastructure, service and support potential issues and concerns with all parties.
- Price and finance the solution that will work for all parties.

- Introduce a powerful transaction profiling system to remove the guesswork from traditional exception reporting tools by automatically pinpointing otherwise undetectable potential losses, to pull it all together.

Why Did I Believe That March Networks Offered the Best Solution?

As I said earlier, from my experience, I believed that March Networks offered the best solution at the time and for the foreseeable future for this type of deployment. I believed and still do, that for many needs, a solution, that a Hybrid Networked Video Recorders (NVRs) that could handle camera feeds from both analog and IP cameras with enough local internal storage (up to 3TB) with Enterprise-class video and audio recording, storage, retrieval and management. The solution had an embedded Linux based operating system. That would support MPEG-4 compression to ensure high bandwidth and storage efficiency. Offer advanced health monitoring, reporting and maintenance tools with Enterprise Service Manager for franchisees with 1+ location(s).

The March Networks hardware gave me many options for the franchisees. We had a 16 analog camera/8 IP camera solution the 4216C, which is rack mountable or wall mountable with 3TB of storage available. We had an 8 analog camera/2 IP camera solution the 3108. And, we had a very small 4 analog/4 IP camera solution, the 3204. The 3204 used by six of the top ten banks for their ATM machines, these worked nicely in their kiosks located in gas stations and other small locations. The 3204 with dimensions of 2.2 in. (h) x10.4 in. (w) x10.3 in. (d) could be installed just about anywhere.

Additionally, in June 2006 March Networks announced their intention to purchase Trax Retail Solutions, Inc. and its affiliated company. Trax was a leading provider of enterprise software for loss prevention, store operations control and profit optimization solutions within the retail sector. I was familiar with Trax's work in the convenience store (C-Store) and grocery store industry. Today March calls the Trax

Solution “Extreme LP” (<http://www.traxretail.com/Resources/Datasheets/16.aspx>). What excited me about this solution is that it pushes the follow-up down to the lowest management level. The Franchisee or his managers receive regular live updates on their cell phones and have a webpage they can access that will show them the 10 most suspicious transactions from their previous shift with links to the video, no searching, no guesswork, just verify.

What is exciting to me is that in the future as Dunkin pulls all their transaction data together. What I mean is that every key-stroke that is available from the Radiant POS solution XML output. We can collect that information into a protected database so clients will be able to compare how a transaction was entered into the system, not just the transaction itself. This will show employees trying to manipulate the system even before they have actually created a fraudulent transaction, eliminating opportunity & temptation.

The Lab Tests

Once the decision was made on which solutions Dunkin wanted to physically test, which were four companies, I was confident that we would win. Why do you ask? First we were the only Linux embedded solution, which was a key benefit for me and most of the IT department at the Brand. Next, we were the only pure enterprise wide network hybrid solution that could be a clean upgrade for franchisee so they could use some of their existing systems such as their existing cameras. The competition was one of my previous employers using Windows based servers. The second competing company was offering older DVR technology but, not offering real enterprise capabilities for the franchisee. Finally the last vendor was a new, unproven, very advanced IP Software-as-a-Service (SaaS) solution using IP cameras and high monthly reoccurring fees.

My biggest issue in the lab tests was to convince March Networks to do the software development needed to prove the solution without a financial commitment from the 'Brand'. However, we got thru that bump in the road and were approved for the next test, the trials.

The Trials and the IT Sub-Committee

Finally, I was able to meet the Franchisee's involved in the decision. The initial 10 locations gave us a good mix of situations and store types. We found that many Franchisees did not always do things as they did them at the lab. We needed to make a few adjustments in the software. I created some basic searches that enabled the software to find theft within all of the stores. But, more importantly I was able to teach some basic procedures that have worked since remote video access was possible. I taught the Franchisees and their managers to log into the stores 4-6 times a week, find something positive and then call the store on the phone and speak to the employee. Discuss the positive behavior such as: "Hi I see you have been very busy tonight, I just want to tell you that you are doing a great job for me." Then I would have them give some direction like "I see that there are some papers blowing around outside. Can you have someone go out and pick them up?" "Thanks again for all your good work." Comments like these have a very powerful psychological impact on the staff. They assume that the Franchisee is sitting somewhere 24/7 watching the store on video. They talk about it among themselves and stop stealing, give better customer service and basically just do their job. Remember, at most locations we already had terminated someone for theft within the first week so everyone got the message. The calls kept the idea fresh in their minds. This has always been the real power of video surveillance, to remove the opportunity and temptation from the store. I have always lived by the concept that "Operations Management" is defined for me as doing things right and "Leadership" is doing the right things.

In Conclusion

In September, 2006 I submitted my proposal to Dunkin' Brands, it was over 500 pages of proofs, processes, procedures and detailed documents and pricing. The decision to deploy the March Networks system was not made until April of 2007 and real deployment did not ramp up until the early 2008. Changes in corporate personnel at the Brand and political issues within the Franchisee Organization kept everyone in the test, re-test and trial mode. The biggest reason, I believe, was that nobody could believe the financial results were real. Everyone had to see it and try it for themselves. I spent a good three months on a plane traveling from one franchisee to another demonstrating or overseeing the installation of the test systems, training and building a political following. We had about forty locations installed before we began to gain some critical mass from the franchisee organization and people started to trust the results that other franchisees were experiencing, many did not believe what they were hearing. A few months later Dunkin Corporate started running their own comparisons between locations using our new system vs. other video systems and the results spoke volumes.

Today, if I was doing it all again I might recommend March Networks and then again I might not. I would still look for the level of integration I had with March Networks/Trax, but I would probably want more capabilities such as: access control integration on the doors; integration of more video analytics, especially behavioral analytics.

Most systems pay for themselves within 60 to 90 days. Every day a franchisee waits to install a system is costs both them and the franchisor thousands of dollars. To be successful with today's technologies you must remember that the solution needs to become part of the consciousness of the store. The management and employees must change their policies and procedures and habits to reflect the use of the new system. If not, the changes in behaviors will only be temporary and the solution investment will be wasted.

Contact Information

James McDonald,

Physical Security Consultant

MassBiz, LLC

109 Bay Path Road

East Brookfield, MA 01515

P/F: (877) 214-2900

M: (774) 239-1128

Email: Jamie.mcdonald@massbiz.com

Consulting Website: <http://www.massbiz.com>

Blog/Community: <http://physectech.org/main/summary>

Client Website with Links & Solutions: <http://www.physicalsecuritytechnologist.com/home>