The COOPERATOR®
The Co-op & Condo Monthly

Data Security

Protecting Yourself & Your Applicants

By Steven Cutler

If they have a mind to, an unscrupulous person in possession of someone's personal information can cause a lot of damage. Their mischief can range from opening charge cards and other lines of credit, running up huge charges in the victim's name that go unpaid and wreak havoc on his or her credit rating, to emptying bank accounts. All a criminal needs is an individual's name, address, social security number and bank account numbers.

Where might such information be gathered together in one neat package?

"Co-op applications are probably the most invasive request for documents and personal information that a person will have in their lifetime,"

observes Stephen Elbaz, president of Esquire Management Corp., which manages co-ops and condominiums in Brooklyn, Queens and Manhattan. “It’s really more invasive than a typical bank loan, which deals strictly in financial information.”

The co-op package is a smorgasbord of private information, including, in addition to Social Security and bank account numbers, copies of checks, the signature on which can be copied, and personal reference letters. And the shareholder approval process always includes a credit report, which provides a list of credit cards and where they have been used.

Whodunnit?

Identity theft and fraud is a particularly insidious crime, not just for the damage it does financially and psychologically, but because of the difficulty to tie perpetrators to the specific data breach event. Victims are commonly unaware of the misappropriation until long after the damage has been done.

According to a report by the Federal Trade Commission, "Determining the link between data breaches and identity theft is challenging, primarily because identity theft victims often do not know how their personal information was obtained."

At first blush, a study issued by Carnegie Mellon University looks encouraging, finding that the probability of becoming a victim of identity theft due to a particular data breach is only around two percent. But the scope of these instances of data breach puts that figure into grim perspective.

In 2007, TJX, the Massachusetts-based owner of the T.J. Maxx and Marshalls discount chains, said that hackers had broken into its computer systems and stolen about 45.7 million credit and debit-card numbers. The TJX breach, which came to light in 2007, was caused by incorrect storage of credit and debit card data, in violation of the Payment Card Industry Data Security Standard. Investigators determined that a hacker had stolen information from the Framingham, Massachusetts-based company dealing with 45 million accounts, starting in 2005 with some going as far back as 2003. A class-action lawsuit resulted in the company paying tens of millions of dollars to affected customers. The settlement with 41 states’ attorneys general resulted in a $7.5 million payout.

The intense media coverage of the mammoth data breach shook up the citizenry of Massachusetts and prompted the state legislature to draw up one of the toughest data protection laws in the nation, and, perforce, one the most onerous for businesses, institutions and organizations to comply with. Indeed, while the law was passed in September 2008 with a deadline for compliance of January 1, 2009, vociferous protests from business groups, non-profits and colleges and universities forced lawmakers to kick the date of compliance way down the road.

The deadline was postponed three times, until it finally went into effect March 1, 2010. And while they've had nearly three years to prepare, businesses and organizations are still struggling to comply, risking fines of up to $5,000 per violation for non-compliance.

The new Massachusetts Data Protection Law requires each and every entity which keeps personal information about a Massachusetts resident to implement a comprehensive information security program, even if the business or entity does not have offices in the state.

Corporations must collect and maintain written security policies and keep a detailed inventory of all personal data and where it is stored, whether on electronic media or on paper. Any organization which handles sensitive personal information on citizens of the state must encrypt that data as it is transmitted over the Internet or stored on external mobile devices such as laptops, flash drives and other mobile storage equipment. Each is mandated to draw up a written security program detailing their how they handle personal information.

Companies big and small in Massachusetts, one of only two states (the other being Nevada) that require companies to encrypt data sent over the Internet, are scrambling to determine how they will comply with the new regulations.

Co-ops & Condos, This Means You!

One thing is certain: the new law applies to co-op and condominium management and officers. According to attorney Moira Casey, director of human resources with the law firm of Marcus, Errico, Emmer & Brooks, PC in Braintree, MA., "Property managers need to start preparations to ensure compliance with the regulations."

The Massachusetts Office of Consumer Affairs and Business Regulation has

estimated that the average small business with 10 employees will need to spend about $3,000 up front on the required software and up to $500 a month for ongoing administration, while bigger organizations could end up spending hundreds of thousands of dollars. Companies will also be required to deploy up-to-date firewalls to create “an electronic gatekeeper” between the data and the outside world that only allows authorized users to access or transmit data.

Hello New York

Data fraud is a crime that is not going away soon. And according to regulatory compliance expert Agnes Bundy Scanlan, Esq., chief regulatory officer of Boston's TD Bank, and vice chair of the Compliance Management Subcommittee of the American Bar Association, "Given the current climate of consumer protectionism, I think this law will gain attention, and not just in the state."

There are already some state-mandated measures in place in New York aimed at protecting social security numbers, most notably the Social Security Number Protection Law, which sets limits on how an organization uses social security numbers for internal purposes and in their communications with the public. But few management companies and their legal departments, let alone co-op and condo boards of directors, have even heard of them.

Ignorance of the current regulations might not seem like such a big deal at the moment because they have not been enforced. But co-op and condo managers and boards in New York could find themselves facing data protection regulations with teeth sooner than they think. A breach of data in the state anywhere close to the scope of the events in Massachusetts could put a quick end to complacency in the New York State legislature and law enforcement.

In any case, as stories of data crimes come in from states around the country, building managers are apt to face increased concern and pressure from shareholders and prospective owners about the protection of their precious personal data.

Getting Started

It is never too early to start building data protection systems. And keeping a shredder in the office — the “system” on which all-too-many co-op associations rely — hardly counts, say the pros. Eric Goidel of the

Manhattan-based law firm of Borah, Goldstein, Altschuler, Nahins & Goidel PC, an attorney representing over 100 co-ops and condominiums, offers some measures co-ops should take immediately:

“Like in a basketball game, you have to control the number of ‘touches,’” explains Goidel. “It's vital to control who gets to view the applications and who in management gets to process the application.”

“The building must maintain at least one copy with all of the information,” he says, “because for example, if you ever get a Human Rights Commission complaint because you turn somebody down, one of the first things they’ll ask for is the files for everyone you have approved.” But all copies of the application package except for that original should have all personal and private information redacted.

Better still, Goidel suggests that management prepare what he calls a “lease abstract” to distribute to the members of the board’s admissions committee. The manager would give the committee members a copy of the application folder containing only the details they need to evaluate the applicant and to formulate questions for the interview. Even then, each of the copies of the folder are shredded after the interview. Ideally, the manager will scan the original documents into a computerized database, protecting it with a password shared with very few staff members at the management company. To tighten security even further, the prospective purchaser can be required to submit the data electronically, so no hard copies exist.

Elbaz recommends that boards ask applicants to take security into their own hands from the outset. They should send management one copy of an application containing private data, and then on the copies they send to the co-op or condo association, “They should black out everything but the last three or four digits of their bank accounts and then make a photocopy of it, because many times people can hold that piece of paper up to a light and see the number. Make it impossible to see.”

Secondly, he recommends the prospective shareholder bind application documents into a book, using VeloBind or some other type of binding system available at Staples or FedEx Kinko's. “It makes it less likely that individual sheets of paper with sensitive information will fall out of the folder and get lost.”

If the applicant is concerned these extra precautions might offend board

members, making it seem as if the applicant is challenging their trustworthiness, Elbaz suggests they enclose a cover letter saying explicitly, "'I am a reliable and responsible person who would be a good asset to the building and as such I have redacted my information.' The cover letter explains that since you are a responsible and good person this is one of the ways you live your life responsibly."

The Basic Data Protection System

If a co-op and condo manager owns a computer and scanner, they already have the hardware necessary to set up a basic yet sophisticated data protection system. All they need is data encryption software to protect documents scanned into the computer.

Dozens of software programs are available that provide high-level password-protection for data stored on desktop computers, laptops and removable storage devices. Symantec, one of the largest companies in the computer data protection field, offers encryption products for $150 and less per end user per year. The cost increases according to the size of the files management needs to store and the number of devices that need to be protected.

Another data protection approach is to keep all records in the "clouds," on Internet servers. For example, users of the Internet-based property management company BuildingLink.com can upload documents containing sensitive information, protected by a password specific to that document. According to the company's president, Jerry Kestenbaum, "A board member can be authorized to look at that one document using the co-op board password. The system tracks who clicks to open it and when."

Servicing primarily high-rise luxury apartment buildings, BuildingLink is pricey, but Kestenbaum suspects there is another reason some buildings don't use Internet-based services: "Most managing agents don't go the online route for the simple reason that if they are doing the same thing that everyone else is doing, if there is a security breach, at least they can say in their defense, 'Well we just did what everyone else does.' "

But they needn't worry. According to Goidel, "As long as they are exercising reasonable care, the director's and officer's liability insurance will cover any claim that may arise, but that's little solace to the shareholder or unit owner whose life is turned upside down by a data breach. Just because there's not going to be any significant financial exposure to a board member or entity doesn't mean that they shouldn't take the utmost

precautions."

Steven Cutler is a freelance writer and reporter living in New York City.