ACT SMART I.T.
www.ACTSmartIT.com
General Business Edition – June 2024

Fraud: How to Protect Yourself

At a recent Cape Cod Canal Chamber event, I met Vincent Pircio, the Branch Manager of Rockland Trust in East Wareham. He's been the manager there for two years. We talked about scams, and he has seen so many! Although there are some really crazy ones where a client thinks they are having a relationship with a celebrity, here are a few of his more common experiences.
~Pam

In a world where technology is growing at an alarming rate, where we do the majority of our business online, it is more important than ever to be aware of the many scams that are out and about. Cybercriminals are constantly coming up with new and deceiving ways to manipulate individuals and create anxiety to try to scam us out of our hard-earned money. Understanding the ways that these criminals operate and the different methods that they will use to commit fraud is the best way to prevent ourselves from being a victim of fraud. This article will elaborate on some common scams we are seeing every day, what to look out for, how to protect ourselves, and the steps to be followed after we suspect fraud.

The "Family Member in Trouble" scam

One of the most common scams that we see in the banking world is the "Family in trouble" scam. You will get a call from a scammer who will pretend to be a loved one. They will tell you that they were arrested and not to tell anyone else in the family and tell you that you need to wire funds to them so they can post bail. As soon as you send the wire, your funds are gone.

You have been hacked scam

Another common scam we are seeing at least once per week is the "your computer is hacked so call Microsoft to resolve" scam. What happens in this scenario is you will get a pop-up on your computer indicating that your computer has been compromised, and you need to call a number to get it fixed. They will tell you your entire system is compromised, and that they will transfer you to your bank's fraud department. They will then instruct you to go to the bank and withdraw cash, take that cash to a bitcoin machine, and enter all of it in and send the funds directly to them. Once you put your money in this machine it is gone.

Payment for Advertising Scam

The final scam we will review is the "advertise for us" scam. In this scam you will receive a check in the mail that you were NOT expecting. The check will include a letter that will tell you that you have been selected to advertise for a large corporation,

Continued on Page 3

From The Desk of David Snell

8 ' «« ‰ # > · ¡ m –

We're looking forward to a fun summer! The grandkids are psyched after having a banner school year! And, their basketball team won the playoffs!

Our hydrangea are loaded with blossoms, the peonies have never had so many flowers and I'm experimenting with llama poop as fertilizer, if you can believe it! We'll let you know how that works out in the Fall.

We're pleased to introduce Vinny Pircio, a fellow member of the Cranberry Country Chamber and the Cape Cod Canal Chamber. Pam met Vinny at a chamber event and shared "Scammer Stories." It was then that she thought that others might want to hear about what he sees at the bank all the time; these aren't just stories made up to scare you, they're honest-to-goodness true-life situations!

We asked Vinny to provide a "Scam of the Month" so we can all see what's really out there and what we need to avoid. We have one more thing to add to Vinny's information:

Don't Blame The Victim!
Blaming victims of cybercrimes, such as falling for phone scams or phishing emails, is common. Society often focuses on what the victim didn't know or do rather than on the criminal's actions. This leads to "fraud shame," where victims feel responsible for the crime, even though the real blame lies with the perpetrator.

Anyone can fall victim to cybercrime, regardless of age, education, or tech skills, as cybercriminals use increasingly sophisticated tactics. Instead of blaming victims, we should focus on understanding these tactics and empowering individuals with the knowledge and skills to stay safe online.

If someone you know is a victim of fraud, don't blame them. Help them contact the authorities (https://www.ic3.gov) and teach them how to recognize phishing attempts and adopt basic cybersecurity practices.

Enjoy the debut of summer!

Always at your service,

(Continued from front page)

a common one I see is Starbucks. They tell you to deposit the check and a portion of the check needs to be sent back to them to pay for the advertising materials, the remainder of the funds are yours. They have you send the funds and then the check comes back fraudulent and is deducted from your account, leaving you with a negative balance.

How can I protect myself?

Now that you know a few different scams fraudsters are attempting and some of the common methods that they will use to gain your trust it is important to review the best things you can do to protect yourself, your information, and your money.

Stay Calm!

These fraudsters use your emotion to get you anxious, flustered, angry: Whatever it may be, it doesn't matter! They just want to get you emotional so you don't think clearly. If you get an alert that you are being scammed the very first and most important thing you can do is STAY CALM.

Hang up Immediately!

Part of using your emotion is to get you to trust them. They will tell you that they are the only ones that can help. This is a lie! If they are over the phone, hang up on them immediately. Even if they are claiming to be from your financial institution, or Microsoft, or Starbucks, hang up and call someone from your bank that you know and trust.

It's important to mention that these scammers are so advanced they can even spoof a phone number. They may even call you from your bank's customer service number. It is still best practice to hangup and call someone you trust.

Never trust a pop-up!

One of the ways these fraudsters will get access to your computer is through pop-ups. Pop–ups open the door for scammers to get into your computer. Once they are in your computer, they have access to just about anything and everything. If you saved your tax return on it, they have access. If you had your username and password for your online banking saved, they have it now too. Avoid pop-ups at all costs!

If you end up allowing the scammers to get this far, remember the rule tip: Stay Calm. If you get one of these pop-ups, we highly recommend having your computer scanned by a professional. These fraudsters are capable of leaving programs in your computer to get data even after the fact.

Trust your local banker!

Do you think there's even a SLIGHT chance someone is trying to scam you? As your local banker, we see these scams on a daily basis, and we know exactly what steps need to be taken to resolve the fraud if you were scammed, or even better, how to prevent it from happening in the first place.

In this digital world, it's never been more important to protect yourself and your information. I hope this article will help many people avoid being scammed and keep their hard-earned money safe!

Vincent A Pircio, Branch Manager II,

Rockland Trust

2995 Cranberry Highway, East Wareham, MA 02538

Phone (508) 295-6900 | Fax (508) 295-7178

Vincent.Pircio@RocklandTrust.com

Vacation Time Anyone?

Despite these dreary and rainy days, this is an ideal time for employers to think about their vacation policy and perhaps provide clarification to employees who may be confused as to how and when they can take their days.

Policies generally serve as a communication tool for businesses. Employees want the ability to refer to a policy to find out exactly what their employer is providing. Vacation is certainly an area where there should be no misunderstandings.

Are you one of those VERY FEW employers that doesn't provide vacation? After all, it isn't required under Massachusetts law. That's right. Vacation is not a mandated benefit for private non-unionized employers in the Commonwealth.

Then why do you have a vacation (a/k/a PTO) policy? Why have you been counseled about the importance of providing such paid time off? The answer includes the fact that most job seekers "expect" to have PTO. And, paid vacation not only addresses the needs of recruitment, but also helps to maintain your existing valued employees. Generally, employers want a workplace where their employees are not completely burnt out! Consider the fact that providing a vacation benefit reduces employee turnover. It also supports employee work-life balance.

Is it always possible for an employer to offer vacation? If you have a snowplowing business, your concern would be having sufficient staff for the winter months. If it is a seasonal business, and you are hiring employees solely for your busy season, it may be a situation where vacation is not offered.

Assuming you have a year-round business and you are in the majority of employers who do provide vacation time, you may set limits on when vacation time may be utilized based on the needs and demands of your business.

For example, do you traditionally have a "busy season"? Florists and candy shops are usually very active in the weeks leading up to Christmas and the time before Valentine's Day. Can you have a policy that states employees will not be granted vacation time during those periods? YES.

These parameters, however, must be set forth IN ADVANCE, so that employees understand those restrictions. Ideally, this policy should be provided when an offer of employment is made. Or, if you implement the policy at another time, post-hire, it's only fair to provide sufficient notice to the employees.

In the case of the snowplow business, where there may be other year-round duties, consider letting the employees know during the summer of 2024 that there will not be any vacation time granted during January or February 2025, so that they are not blindsided in 2025 and can make appropriate plans for vacation during other months.

Although vacation is not required, when an employer offers paid vacation days to an employee in an offer letter, in their policies, as part of a contract, or as part of a written agreement, those paid vacation hours are considered "wages" in Massachusetts.

The methods of providing such paid time off vary. Businesses may have employees earn / accrue vacation days, typically on a monthly basis. You may choose to have an employee complete an introductory period before allowing the accrual or the use of available days. Or, you can provide a frontload or lump sum of days or weeks at the beginning of a calendar year or upon the employee's anniversary year.

In choosing a method of providing vacation time, employers MAY consider whether applicants for employment expect access to time off on a more immediate basis rather than waiting for a few hours or days to be accrued each month. But some employers may not be comfortable providing a liberal number of weeks to a newer employee. Perhaps that "privilege" would be extended to longer-term employees (i.e., frontload for those employees with 3+ or 5+ years in the Company. Another consideration is the requirement that employers must pay employees for all accrued unused vacation at time of separation from employment, whether the separation was voluntary or involuntary.

What is a "use it or lose it" policy? This type of policy would require your employee to use their vacation time within the year it was accrued (the anniversary year or the calendar year, whichever your business uses for providing these employee benefits). An employee who fails to use the vacation time would lose that paid benefit. As an alternative, you can implement a policy that allows the employee the ability to "carry over" *some* of the unused vacation but lose the remainder.

In addition to the vacation hours an employer allows, some businesses close for certain weeks during the year and give those weeks as "paid vacation" to staff. It is common for employers to close the week of July 4th, as many businesses find that to be a slow week (except for entities in vacation areas, such as stores or restaurants at the Cape!). Similarly, some employers close for the holiday week in December. Providing employees with paid time off during those weeks is sometimes referred to as "forced vacation."

Employers may set up their own procedures for the vacation request and for scheduling. It is important to retain the right to determine whether or not to approve the request for time off. Always use objective factors to make that determination, which might relate to the needs of the business during the requested period of time.

A reminder that vacation time that is provided as a benefit is viewed like earned wage. Employers may not hold back vacation payment as a disciplinary measure. In Massachusetts and many other states, it must be paid at time of separation from employment, whether that separation is voluntary or involuntary.

To properly track sick time and manage vacation time, some employers prefer to keep "separate buckets" while other role the time off into one category of Paid Time Off (PTO). There are pros and cons to both approaches.

When you revise your handbook or other policies, you may choose to re-think your vacation policies and adjust those provisions accordingly. As with any aspect of the interpersonal human resources function, communication as to your policies and expectations in terms of vacation is key.

Attorney Helene Horn Figman combines specialized legal knowledge in employment law with the skills and perspectives uniquely suited to Human Resources Consulting. www.figmanlaw.com

Information about her anti-harassment and anti-discrimination education programs can be found at www.workplaceawarenesstraining.com

This article has been prepared by the Law Offices of Helene Horn Figman, P.C. for general informational purposes only. It does not constitute legal advice and is presented without any representation of warranty whatsoever.

Helene Horn Figman

Law Offices of Helene Horn Figman, P.C.

Employment Law & HR Resource Management

45 Bristol Drive Suite 207, South Easton, MA 02375

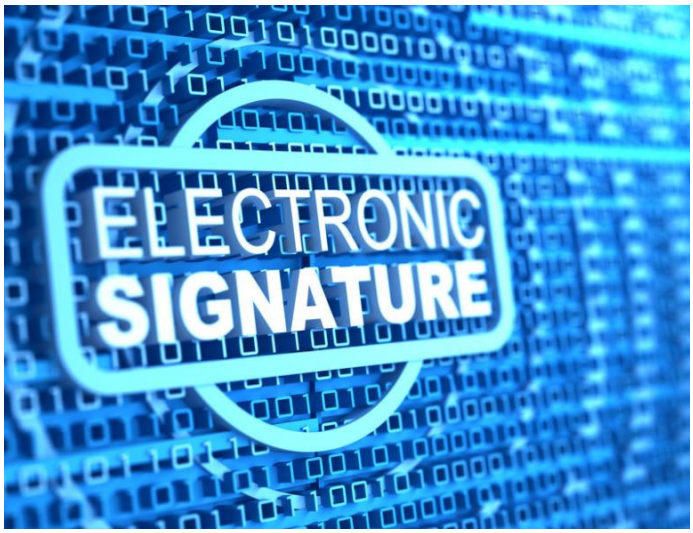
FigmanLaw.com hfigman@figmanlaw.com

508-238-2700

How Much Choice Does Your Industry Have

A lot of businesses and organizations have the luxury of shopping around when it comes to selecting an eSignature provider. However, depending on your region and industry, this isn't always the case. In this article, we look at those exceptions.

All businesses must comply with federal eSignature regulations.



No matter what industry you're working in, you must select an eSignature provider that complies with federal regulations. In the United States, that includes:

- The Electronic Signatures in Global and National Commerce Act (ESIGN) – a federal law that was enacted in 2000 with the purpose of facilitating the use of electronic signatures and records in interstate and foreign commerce, establishing the legal validity and enforceability of electronic signatures, contracts, and records, and ensuring that they have the same legal status as their paper counterparts.
The Uniform Electronic Transactions Act (UETA) – a federal law approved in 1999 with the goal of creating consistency in electronic commerce laws across states.

Businesses operating within the United States must also adhere to any state regulations that apply.
For organizations operating in Canada, on top of any provincial electronic commerce acts, these regulations include:
The Personal Information Protection and Electronic Documents Act (PIPEDA) – passed in 2000, this act governs the collection, use, and disclosure of personal information, including eSignature.

Why are some industries limited to certain providers?
Due to the sensitive nature of some materials that might be dispersed via eSignature, some industries have specific provider requirements that limit an organization's ability to be selective about their vendor if they wish to remain compliant.
Some industries that often have specific regulations or standards governing the use of eSignature providers include:

- Healthcare providers.
- Banking and financial services.
- Government.
- Legal services.
- Certain types of insurance providers.
- Real estate businesses.
- International trade and commerce.
- Aerospace and defense manufacturers, contractors, etc.

Often, due to the nature of the work being done in these industries, businesses and organizations have stricter eSignature requirements. We're going to look at some of those requirements across a handful of these industries.

Healthcare
While there isn't a specific list of approved eSignature providers, North American healthcare providers must carefully evaluate potential solutions to ensure they meet the specific legal and regulatory requirements. These regulations are in place to ensure the security and privacy of patient information.

In the United States, the main regulation governing healthcare and eSignature is the Health Insurance Portability and Accountability Act (HIPAA) – which dictates the electronic transmission of healthcare information. Therefore, any healthcare practice or business dealing with healthcare information must ensure the eSignature provider they use is HIPAA compliant.

Some of those specifications include:

- User authorization/authentication.
- Prevention of digital tampering.
- Non-repudiation.

Control over document ownership.
Likewise, across the continent, healthcare businesses must also ensure their provider adhere to high-security standards to protect against unauthorized access and data breaches.

When it Comes to Choosing an eSignature Provider?

Banking and finance.
eSignature is complicated in the finance world, with several laws providers must comply with, especially in the United States. On top of the overall federal regulations, financial institutions and businesses must ensure their solutions are compliant with the following:

- The Gramm-Leach-Bliley Act (GLBA) – a 1999 act that requires financial institutions to implement measures to ensure the security and confidentiality of customer non-public personal information.
- The Fair Credit Reporting Act (FCRA) – a 1970 legislation applicable to any organization involved in credit reporting, which includes requirements for consumer consent and disclosure.

Securities and Exchange Commission (SEC) regulations – the SEC governs companies like brokerages, which may have specific regulations for the use of eSignatures in financial transactions and client interactions.

Regardless of your location, it is critically important for financial institutions and businesses to ensure their eSignature provider maintain incredibly high high-security standards to protect against fraud, unauthorized access, and data breaches. Likewise, they must offer robust compliance documentation and audit trails to demonstrate adherence to regulatory requirements. Many organizations will also require seamless integration with existing systems, such as CRMs, as well as compliance with international eSignature requirements, if they do any global transactions.

Insurance
Because of the cross-industry nature of the insurance world, insurance companies often face significant limitations or requirements when choosing eSignature providers. They may be required to comply with healthcare regulations, financial regulations, or more, depending on the products they sell.

When choosing an eSignature solution for an insurance business, it's crucial to not only understand the regulations within your industry, but also governing any adjacent industries as well.

Legal
Like healthcare, legal practices deal with strictly confidential information every day. Therefore, security standards are especially important.
While eSignatures are generally accepted in legal contexts, the requirements can vary based on jurisdiction. For example, certain types of documents like wills, family law documents, or court orders may have specific requirements that not all eSignature providers can fulfill.

What does all of this mean?
It's not necessarily that there's a law out there impeding competition or saying businesses must use 'x' eSignature provider or else. Rather, you might find you're limited as to which providers meet the requirements for your sector. Your organization may not have the same opportunity to shop around as others in different industries.

So how do you be certain you're not getting a bad deal?
With fewer options, it may seem like you have less control over your eSignature plan. However, there are still ways to ensure you're not overspending. A comprehensive audit of your eSignature needs, monthly or quarterly spend, envelope capacity, and more is an important part of optimizing your expenses.

In conclusion…
Different industries that deal in confidential and sensitive information have stricter eSignature requirements and may find they have less freedom when choosing a provider. However, this doesn't mean they have to accept overspending.

Delivering businesses greater profitability by reducing their monthly expenses and adding to their bottom line.

SCHOOLEY MITCHELL

Bryan Berry | Strategic Partner

Tel: 781-427-9595 | Cell: 508-479-7190 | Fax: 781-499-9177
www.schooleymitchell.com/bberry
bryan.berry@schooleymitchell.com

ACTSmart IT
332 Main Street
Wareham, MA 02571

In This Issue:

Would you like to receive our FREE monthly print newsletter? Go to ACTSmartIT.com/newsletters

This newsletter was thoughtfully edited by Susan Rooks, the Grammar Goddess, so we can look and sound as smart as we are.

Susan Rooks
The Grammar Goddess
508 272-5120
SusanR@GrammarGoddess.com

Want to network with the best of them?

This event provides a brief 15-minute outline of "Business to Business Networking Best Practices" followed by 60 minutes of Open Networking o practice your new skills. The live, in-person event is a great oppor tunity to learn a few networking nuggets and then meet new people.

The entire business community is welcome to participate. The compli-mentary B-B networking training and open session is set for Tuesday, June 25, 9:15-10:30 a.m. and will be held at the

Plymouth Area Chamber of Commerce offices
100 Armstrong Road, Suite 204, Plymouth, MA 02360.

Ample free parking is available. Light refreshments will be served.

Other than death, what many professionals fear is "networking" and meeting new people. This complimentary session kicks off with 15 minutes of how to "engage" with someone at a networking event and then how to "disengage" and move on.

The networking ninjas for the session are networkers from birth including Mike Dwyer of Emplana Career, helping professionals expand their horizons, and Steve Dubin of PR Works and founder of My Pinnacle Network, a series of business-to-business networking groups.

For more information, contact Steven Dubin, SDubin@PRWorkZone.com, (781) 582-1061.
Please RSVP to https://rb.gy/mhipul
We'll see you there!