THE IRON CHRONICLES
ENTERPRISE IRON FINANCIAL INDUSTRY SOLUTIONS, INC.

Delivering impactful Business, Technology & Workforce Solutions since 2002.

JULY 2021 | VOL. 2 | ISSUE 3

From The Founders

Nineteen years ago this month, we founded Enterprise Iron to provide superior management and technology consulting services. We watched corporations struggle to gain a competitive advantage for years despite investing heavily in the latest software and platforms, so we knew something was missing. Our aim for Enterprise Iron was to fill that void. Using our expertise, we help clients focus on business strategy and strengthen their understanding of all the products and services in their arsenal. Today, this mantra remains: Expertise. Focus. Strength.

We invite you to join us as we count down to our 20th anniversary celebration next summer and explore EI's past, present, and future in these upcoming newsletters. Enterprise Iron Financial Industry Solutions, Inc. began as a conversation on John's back porch, and we get our name from the large mainframe computers nicknamed "big iron" that serve the enterprise. While some of these mainframes have been retired with time, many continue to function as the infrastructure backbone of our Insurance and Government clients.

New Jersey is our home and headquarters, but we've grown a lot over the years. Today, we have over 120 employees across the U.S. and Canada servicing clients in 31 states, plus our Contact Center in San Juan, Puerto Rico. Our expertise and reputation for excellence continue to fuel our ability to deliver results for clients across Retirement Services, Financial Services, and the Government sector. We continue to expand our capabilities to bring value and purpose to an ever-changing world and continue to exhibit the staying power like the mainframes EI was named after.

Inside this issue: Tim Scott reflects on years of business change, Paul Gallagher breaks down the DOL guidance on cybersecurity responsibilities for retirement plans and Mark Kalafsky delivers the next installment in his Agile series.

In closing, we want to use this opportunity to thank our clients, partners, employees, families, and friends who have helped make Enterprise Iron what it is today. Our continued success is made possible through all your support. As a small (but mighty) business, we are immensely proud of what we've achieved to date and are excited for what lies ahead.

Best,
John P. Polito & John R. Crocker
Co-Founders

UPCOMING EVENTS

NASRA Conference	Aug. 4th – 11th
NAPA 401(k) Summit	Sept. 12th – 14th
NAGDCA Annual	Sept. 13th – 16th
ASPPA Annual	Oct. 17th – 20th
Wealth@wor(k)	Oct. 24th – 26th

Reflecting on Nearly 20 Years of Business Change

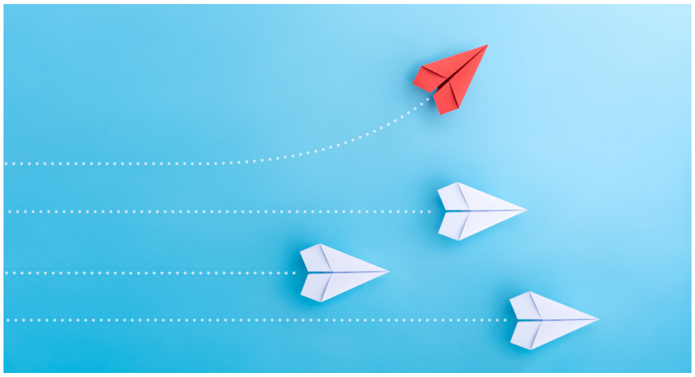
By Tim Scott, SVP of Business Development

Enterprise Iron has undergone many changes and growth since our origin, including the industries we serve, how we provide services, and the depth of our capabilities. When EI began, processing in the Financial Services industry was primarily paper-based with limited automation. In one of our first projects, we digitized the clients' hardcopy files by scanning and organizing them to ease access. Digitization now has a whole new meaning, but EI has been here since the beginning. Strengthened by the background of our founders, EI also quickly became known as a firm with expertise in

Trust and Custody services and helped implement major systems in some of the largest Wall Street firms.

I first became acquainted with Enterprise Iron in 2004 while working for a major retirement recordkeeping software firm. We were engaged in a large-scale implementation, replacing a proprietary platform with our Modifiable-Off-The-Shelf (MOTS) platform. Due to the scale of the program, there was a multitude of resource needs. EI was one of the firms I worked with to provide experienced resources in support of our client. In fact, through their industry contacts and recruiting and onboarding processes, I brought in volumes of resources on short notice. EI quickly became my "go-to" partner as our business grew and this time represented a significant step for Enterprise Iron's growth into the Retirement Services industry.

In 2008, the world was shocked by the financial crisis, and EI was not immune to the effects as our clients had to cut budgets and reduce spending. Companies sought to control costs and compete in a world where margins were suddenly cut by half or more. We understood these challenges and had proven experience in Business Process Reengineering and Automation using industry-standard tools and applications to help.



During the years that followed, EI continued to focus on private clients in Retirement and gained recognition as a firm that was an essential player in the industry. We invested in our team and capabilities to meet the demands of an ever-changing world of increased regulation, required automation, and the modernization of aging platforms. That investment paid off in 2013 when a major managed services contract was awarded to Enterprise Iron to provide technology and operations for the retirement plan servicing all Federal employees. This opportunity pushed EI to accommodate the needs of our largest client. Ever since, we've expanded our service catalog, developed partnerships, and entered new markets. Today, we provide a full suite of technical and operational services to meet the needs of global and domestic Financial Services firms, public sector agencies at the federal, state, and local level, Retirement Plan Sponsors, Advisors, and Providers.

We offer Managed Services of technology and operations, Platform & Provider Search as a truly independent partner, Platform Modernization using technology enablement tools, and Business Process Reengineering consulting. Our expert Custom Development, Business and Technical Analysis, QA Testing, Test Automation, Program & Project Management, Agile Development, and Implementation Services of vendor platforms round out our deep corporate capabilities. We leverage our secured, 2,000 seat Contact Center in Puerto Rico to provide overflow and primary call center services through our Rightsourcing solution.

As the needs of our industries evolve, Enterprise Iron continues to invest for the future. We are investing in Cloud technology and solutions to assist our clients with migrations. We're also developing a Digital Transformation Implementation solution and a Cybersecurity Assessment and Implementations offering.

Enterprise Iron has grown significantly since our founding and continues to adapt to deliver impactful results for clients. We are committed to staying on the cutting-edge of change for whatever the future holds, and if your organization is seeking a trusted partner to help navigate business change, give us a call.

THE RESTATEMENT PERIOD IS OPEN FOR PRE-APPROVED DEFINED CONTRIBUTION PLANS.

Our Plan Restatement & Operational Consultants are ready to support your team and keep your organization compliant!

THE IRON CHRONICLES
ENTERPRISE IRON FINANCIAL INDUSTRY SOLUTIONS, INC.

Delivering impactful Business, Technology & Workforce Solutions since 2002.

JULY 2021 | VOL. 2 | ISSUE 3

C	D	S	V	W	X	G	O	C	M	A	Q	N	C
O	G	Z	Q	L	R	M	L	J	Y	P	R	O	X
N	E	S	I	T	R	E	P	X	E	E	F	I	T
S	O	V	E	P	T	S	P	R	C	L	V	T	M
U	T	P	R	X	Y	J	A	O	R	A	X	S	D
L	T	M	I	M	P	T	R	A	E	F	T	Z	F
T	P	V	S	K	I	D	S	G	T	V	X	I	I
I	B	E	A	O	K	F	C	I	I	B	N	N	D
N	P	W	N	E	R	X	T	L	R	L	N	R	U
G	F	S	E	S	D	Y	D	E	E	A	C	E	C
H	D	P	R	Y	I	A	A	Q	M	A	B	D	I
V	E	S	L	W	T	O	H	S	E	L	X	O	A
R	H	I	P	A	W	G	N	R	N	A	O	M	R
I	C	C	A	R	E	S	A	C	T	V	P	P	Y

Word Bank:

RECORDKEEPER
FIDUCIARY
EXPERTISE
PENSION
OPERATIONS
CONSULTING
MODERNIZATION
RETIREMENT
CARES ACT
ERISA
AGILE
DATA

Cybersecurity: Another Responsibility for Retirement Plan Sponsors & Fiduciaries

By Paul J. Gallagher, Managing Director of Plan Sponsor Services

Cybersecurity is the art of protecting networks, devices, and data from unauthorized access and unlawful use. An integral component of a cybersecurity program involves ensuring the accuracy, integrity, and availability of information. The ability of the U.S. Government, Fortune 500 firms, and public and private companies to craft and execute effective cybersecurity policies, processes, and procedures is a daily challenge that costs hundreds of millions of dollars annually.

Yet, headlines are full of stories detailing massive data breaches involving the passwords, ids, and SSNs of millions of people. There are often far more severe situations like the recent ransomware attacks on Colonial Pipeline and JBS, the second-largest meatpacker in the world.

The interconnectedness of the technology we rely upon also enables a small number of bad actors to wreak substantial damages on firms and governmental entities. In the process, millions of people have their identity, health records, and critical financial information like retirement, credit card, and bank accounts comprised, or in the worst-case scenario – stolen.

In April 2021, The U.S. Department of Labor issued new **guidance for plan sponsors, plan fiduciaries, recordkeepers and plan participants** on best practices to establish, enhance and maintain cybersecurity for the $9.3 Trillion held in DB and DC plans.[1] The objective is to protect the retirement benefits of the 140 million American workers covered by these plans.

The timing of this guidance was interesting. It came shortly after a Government Accountability Office **(GAO) report** was issued in February 2021.[2] That report highlighted the risks of sharing Personally Identifiable Information (PII) such as SSNs, DOB, retirement account, and bank account data through the mammoth IT infrastructure within the retirement plan ecosystem. Risk can emanate from different sources and take various forms. The GAO report included two recommendations:

1) The DOL should formally state if cybersecurity for ERISA is a plan fiduciary responsibility

2) The DOL should develop and issue guidance that identifies minimum expectations for mitigating cybersecurity risks to plans and service providers that administer plans

The DOL took the GAO recommendations seriously and provided guidance. They also made it clear that cybersecurity is a plan sponsor responsibility by indicating that ERISA's duty of prudence encompasses "an obligation to ensure mitigation of cybersecurity risks."[3] The DOL guidance, created by the Employee Benefits Security Administration (EBSA), addressed the key constituencies within the retirement ecosystem:

- Plan Sponsors and Plan Fiduciaries
- Recordkeepers
- Participants

The guidance helps plan sponsors, fiduciaries, and plan participants "safeguard retirement benefits and personal information."[4] The DOL was explicit that their view is the guidance "emphasizes the importance that plan sponsors and fiduciaries must place on combatting cybercrime."[5]

The guidance features *Tips for Hiring a Service Provider*, designed to help plan sponsors and fiduciaries select providers with robust cybersecurity capabilities. A *Cybersecurity Best Practices* document aims to help fiduciaries understand and manage their cybersecurity responsibilities. Also included is an *Online Security Tips* factsheet for participants.

- The *Tips for Hiring a Service Provider* is a valuable document that recommends asking questions about a firms' policies and track record. You should also ask about previous breaches, if any, insurance coverage, and the procedures for using, storing, and sharing participant data.
- The *Cybersecurity Best Practices* information is targeted at recordkeepers and other service providers and is a compendium of what a provider should have. It covers everything from access controls to disaster recovery and independent threat assessments.
- The *Online Security Tips* recommends a series of practical steps a participant can take to protect their information.

It is noteworthy that the *Tips for Hiring a Service Provider* and the *Cybersecurity Best Practices* guide do not address if these rules impact current service providers. It is our opinion that the DOL believes they do, and therefore, plan sponsors should review these guidelines with their current plan provider.

Should you or your plan committee need assistance understanding cybersecurity or how the regulations impact your retirement plan, Enterprise Iron is here to help! We've worked with public and private plans of all sizes, plan types, and the service providers who support them. We provide an independent, objective assessment of your plan and service providers' compliance with the new guidelines to identify any areas of improvement. Enterprise Iron will work with you to implement any needed changes.

Turning Up the Heat

While the guidance lacks the weight of regulation, immediately after it was released, there were reports that the DOL launched a series of inquiries about retirement plans' cybersecurity practices. There are also reports that the DOL audit process now includes questions about the cybersecurity practices, policies, and procedures that a plan sponsor or their service providers apply to the plan.

It is hard to imagine what comes next. Still, the focus on cybersecurity implies that the DOL will start to hold plans and their fiduciaries accountable for cybersecurity. Besides the specter of a DOL enforcement action, this guidance should remind plan sponsors that if a cybersecurity breach ever impacts their plan, they need to be prepared. Class action lawsuits that argue that they chose the wrong service provider or that PII was misused or not protected are possible. Service Providers like recordkeepers, TPAs, and advisors will likely be inundated with requests to divulge the precise details of their cybersecurity and information security practices.

What's Next

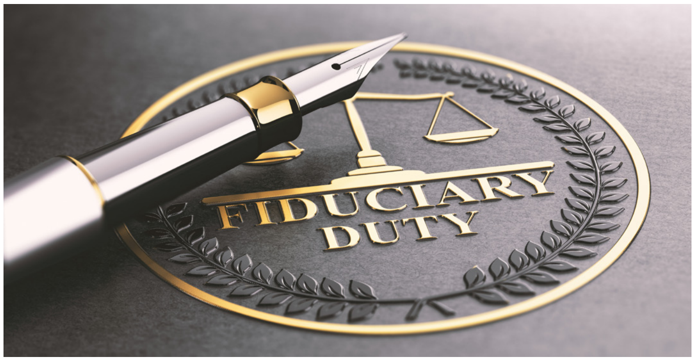
Without question, this guidance is a watershed event. While there are still quite a few open questions, e.g., Must a plan sponsor distribute the *Online Security Tips* to every employee? If so, when? Regardless, the headline is that the DOL has invoked the ERISA duty of prudence to advise plan sponsors andvfiduciaries responsible for combating cybercrime. Understanding the nuances of cybersecurity may not be new for some plan sponsors and fiduciaries, but it is likely to be intimidating for many.

Next Steps

We encourage all plan sponsors, fiduciaries, and service providers to read the new DOL guidance, conduct a detailed review of your organization's adherence to these precepts and review your service providers adherence to these guidelines.

Regardless of your role, Enterprise Iron is here to help. We have a rich history of helping plan sponsors, and service providers comply and adapt to new guidance. Working with our veteran **Plan Sponsor Services** team, you can be confident that your plan and its service providers – from advisors to payroll providers and recordkeepers – understand and carry out their fiduciary duties.

Please contact us if you have any questions about the new Cybersecurity guidance, a fiduciary's prudence duty, or any questions regarding your retirement plan!



[1, 3, 4, 5] U.S. Department of Labor. April 14, 2021. New Cybersecurity Guidance for Plan Sponsors, Plan Fiduciaries, Record-Keepers, Plan Participants

[2] GAO21-25 February 11, 2021. Defined Contribution Plans: Federal Guidance Could Help Mitigate Risks in 401(k) and Other Retirement Plans

The Birth of Agile

By Mark J. Kalafsky, SVP of Solutions & Delivery

The Agile methodology has come a long way since it first peered out at the turn of the century and behaved like a David to the accepted methodology – the mighty Waterfall, the Goliath of methodologies, the benchmark for every technology shop in the IT universe. Walk the halls and sit in any meeting of every Financial Services firm at the time, from the behemoths on Wall Street to the Web startups, and you'd hear from business executives, "When can we get these changes done? They seem trite and should not be a major issue."

The answer, inevitably, was often along these lines, "Well, we don't have the requirements documented. Therefore, there have been no reviews and signoffs, so I can't give you a date." Now on the odd chance that the requirements were published, the answer usually manifested itself as, "We have to fit your changes into other known requirements since we only do releases twice a year," and so on.

The curse of the Waterfall – living in an IT silo of technicians who coded for IT victories and not solving the business problems at hand, had to go – or at least be supplanted by a nimble, integrated business and technology model. Today, that model is known to the world as Agile.

To most IT historians, Agile got its wings in 2000 when a consortium of seventeen like-minded professionals met in Oregon. Coincidentally, this took place about the same time that our founders, John Polito and John Crocker, were launching Enterprise Iron on the East Coast.

Led by Bob Martin, or “Uncle Bob,” who is recognized as the Pied Piper of Agile, the Group of Seventeen had two major goals in mind: minimize the time a working software model gets into the hands of the user community and respond to those users as rapidly as possible. That’s it! Seems easy, no?

However, the climb to modern-day Agile was a road fraught with resistance by most everyone in the legacy IT divisions. Some of the loudest cries came from the Financial Services community, including the owners of the siloes, “All our quality gates have just been run over,” the regulatory and compliance people, “Hey, I can’t tie back the published requirements to the output,” and often the loudest calls, “We are going to get sued to no end and the SEC will have our backsides in a sling!”

The Group of Seventeen plowed ahead in determined fashion, and their next summit, the now famous 2001 Snowbird meeting, resulted in “The Agile Manifesto.” I suspect that Luther and Marx (Martin and Karl), the authors of the two most famous manifestos to date, did not lose sleep over the significance of this new manifesto. For us IT soldiers, the document would soon become the basis for our new marching orders.

The four pillars of the manifesto read something like this:

- *People and their inputs and interactions are significantly more important than the rigid processes, rules, and software that have defined the existing environment.* AKA, silo walls are coming down.

- *Working pieces of software must be developed and demonstrated as soon as possible.* The delivery packages of the day were bound to be rendered obsolete by this bold commandment. No longer is the user demonstration one of the last pieces of the development process. Now it is required that the user community be involved and continually providing feedback in real-time.

- The new paradigm demands that *IT technologists and representation of every possible business stakeholder all huddling in the same room.* Totally verboten before Agile! IT staff quaked in their boots over this, and some still do not believe in this ‘radical’ concept.

- As soon as *a change is agreed to start the development as quickly as feasible.* AKA, what we lovingly refer to today as “sprints.” Change is good! The rigid legacy project plans of yesteryear live no more. Let’s show the users what we can do, especially since the languages, tools, and processes that technicians had to work with were changing. The COBOL mainframe world, the legacy platform that our founders grew up with, was also changing. New tools like C++, Java, platforms like .NET, and something called “The Web” were maturing simultaneously.

Software Development, as we knew it in 2000, was going the same way that landlines, VCRs, and beepers were – straight to the recycle bin. My next article will discuss the uphill battle that the Agile Army fought to make it into the IT mainstream and become recognized as the ‘de rigueur’ method of building software.

Contact us today to learn more about our **Agile expertise and staffing capabilities**!